

The Scholar Journal for Sciences & Technology

ISSN

Print 2794 - 7629

Online 2794 - 4549



North Europe Academy

Journal published by the Danish Arab Center for Future Studies
Copenhagen - Denmark

DACF
Danish Arab Center for Future Studies



The Scholar Journal for Sciences & Technology

The Scholar Journal for Sciences & Technology - NEA /Copenhagen - Denmark

DACF
Danish Arab Center for Future Studies



VOL 4



NO.8

International Standard Serial Number

ISSN (Print) 2794 - 7629

ISSN (Online) 2794 - 4549

The Scholar Journal for Sciences & Technology
International Standard Serial Number (ISSN)

ISSN (Print) 2794 – 7629
ISSN (Online) 2794 - 4549

Vol. 4

NO. 8

Issue date: 29/07/2026

Chief Editor

Prof.Dr.Harith Salman Hasaani

Professor General surgery
Consultant General Surgeon
General surgery
Al-kindy Teaching Hospital
MD PhD FACS
Ministry of health /Iraq
harith_salman@yahoo.co.uk
009647704587777

Deputy Editor-in-Chief

Prof. Dr. Sabah Mohammed Al-Mutoki

Nano Technology and Advance Material
Al Furat Al Awsat Technical University
Dean of the Technical Institute of Samawah
Prof.dr.sabah1972@atu.edu.iq
009647800764040

Research Publications Officer

Prof. Dr. Abbas Nagi AL Imami
Physiological Psychology & Chemistry Sciences
Director of the Danish Arab Center
CEO of Northern European Academy
Science and scientific research
abbas-45@hotmail.com
004571583979



Editorial board members

D.Sc. AIChE Fellow. Al-Dahhan. Muthanna. H

University of Missouri System Curators
Distinguished Professor of Chemical
ChBE) and of Nuclear Engineering (NE)
College of Engineering & Computing (CEC)
Dep. of Chemical & Biochemical Engineering
aldahhanm@mst.ed

Prof. Dr. Ahmad M. F. Al-Khasawneh

Information Systems
President of Irbid National
University of Jourdan
akhasawneh@hu.edu.jo
akhasawneh@yahoo.com
00962797125217

Prof. Dr. Ahmad Yousef Al Yahya

physics
Damascus University
dr.ahmad.alyahya@gmail.com
00963966592029

Prof. Dr. Ahmed Eltayib Mohammed

Dean, Almanagil College for
Medical & Engineering Sciences
ahmedtayib114@gmail.com
00249123625576

Prof. Dr. Adel Sallam Mohamed Haider

Specialization: Artificial Intelligence
Faculty of Engineering - Aden University
adel_ye@yahoo.com
haider.adel@gmail.com
00967777464454

Prof. Dr. Fareed Mohamed Abdulkarim

Ph.D in Transportation Engineering (Civil)
Faculty of Engineering- University of Aden -
Yemen
dr.fareed.abdulkarim@gmail.com
0096772688181

Prof.Dr.Hesham Ahmed Al Sharie

Civil Engineering
Jerash University
mailto:dr.sharie@yahoo.com
00962795868090

Prof. Dr. Isam Abdulazeez Mohammed

Specialization: Physics
Al-Mustaqbal private University
50016@uotechnology.edu.iq
009647702527825

Prof. Dr. Khaled Abdulhalim Haidar

Civil engineering / Structure
Faculty of Engineering Aden university
Dr.khaledrabassi@gmail.com
00967736096024

Prof. Dr.Mahmoud alakhdar Kweider

Dep.of .Immunology
Damascus university
mahmoudkweider60@yahoo.com
00963932589745

Prof.Dr. Majid Raissan Chalab

Physics, Solia state physics /Nanomaterials
Thi Qar University - College of Science
Majidphy2016@utq.edu.iq
009647822323499

Prof. Dr. Eng. Mohammad D. AL- Taha

Industrial Manufacturing Engineering
Faculty of Engineering
University of Jourdan
altahat@yahoo.com

Prof.Dr. Mohammed Mounaf Mohammed

Faculty of science --department of mathematics
Damascus university
Mounaf19640@gmail.com
00963993501032

Prof. Dr. Mubarak Dirar Abd-Alla

Physics Department
Sudan University of Science and Technology
College of Science
mubarakdirar@gmail.com
00249968855227

Prof. Dr. Noori Mohammed Luaibi

Dep.of Biology / College of Science
Almustansiriyah University
Physiology, Endocrinology
sznl@uomustansiriyah.edu.iq
009647901343049

Prof.Dr. Shimal Younis Abdul-Hadi

Microbial Biotechnology
University of Mosul
College of Education for
pure Sciences
Shimal_y@yahoo.com
009647700366914

Prof. Dr.Talib AH. Mousa

Department of Chemistry- Biochemistry
College of Science
Al Muthanna university
shatnawi@just.edu.jo
00964773646626

Prof. Dr. Vesna Karapetkovska Hristova

Department of Biotechnology
Faculty of Biotechnical Sciences
"Partizanska"bb, 7000 Bitola, Macedonia
E-mail: v.primavera79@gmail.com
mob. + 389 71 318 777
North Macedonia

Prof. Dr. Saja Saleh Jabbar Al-Taweel

Physical Chemistry
Alkarkh University of Science
College of Science
sajataweel@yahoo.com
009647736465264

Prof. Dr. Sultan Muhammad Al-Salkhadi

Faculty of science, department of mathematics
University of Kalamoon
Syrian Republic
Ssalkhadi412@yahoo.com
00963957574157

Prof.Dr.Ziad Tarik AL_dahan

Electrical and Electronic Engineering
Medical System - AlFarahidi University
ziadrmt1959@yahoo.co.uk
009647801550228

Prof.Dr. Ihsan Edan Abdulkareem Al Saimary

Medical microbiology molecular immunology
Department of microbiology
University of Basrah--college of medicine
ihsanalsaimary@gmail.com
009647801410838

Associé. Prof. Dr. Verónica Lassalle

Associate Professor and Principal Scientific
Researcher
Chemical Institute of South (INQUISUR-
CONICET)
Chemical Department
National University of South (UNS), Bahía
Blanca
Buenos Aires, Argentina
Hybrid and Applied Nanomaterial's
(NanoHiAp)
E-mail: velassalle@uns.edu.ar
TE: +54-291-4595101 (int. 3534)



Advisory Board

Prof.Dr.Fathi Khalifa elyaagubi
Environmental pollution
Africa University - Tripoli
felyaagubi@gmail.com
00218913735313

Prof.Dr. Hussein Mandeel Ashour
Civil Engineering
Department of Civil Engineering
Al-Muthanna University, hma@mu.edu.iq
009647815190900

Prof.Dr.Mohammed. M. Abu Shquier
Professor of Computer Science
Jerash University
admin@jpu.edu.jo
00962779830983

Prof. Dr. Samir Manhal Karman
Electronic Engineering
Damascus university
samir_mk@hotmail.com
00963955303289

Prof. Dr. Wasfi Mohammad
Physics atomic, Department of Physics,
College of Science, Diyala University
basicsci25@uodiyala.edu.iq
009647702941306

Asso.prof.Dr. Adam Ahmad Farah
Analytical Chemistry
University of Kordofan, , Sudan
adam1974999@gmail.com
00249918037878

Asso. Prof. Dr. Mazin Yaseen Shatnawi
Department of Chemistry
Jordan University of Science & Technology
shatnawi@just.edu.jo
00962798561159

Assoc.Prof.Dr. Talal Khamis Al Wahaibi
Chemical Engineering
A'Sharqiyah University
Talal.alwahaibi@asu.edu.om
0096805180328

Prof.Dr.Feras .R.A.Afaneh
Experimental Atomic
and Molecular Physics, Physics Department
Hashemite University , afaneh@hu.edu.jo
00962795380610

Prof.Dr.Kayed Abed Alfattah
Department of Organic Chemistry
College of Science, Hashemite University
kayedas@hu.edu.jo
00962796400520

Prof.Dr.Rokhsana Mohammed Ismail E
Engineering. Chemistry
University of Aden
stc@aden-univ.net
00967777123518

Prof.Dr.Sattar Abbood Abbas
Material Physics
university of wassit
starabbas@uowasit.edu.iq
009647715883649

Asso .Prof.Dr. Abdalla Gobara
department of Chemistry
University of Dalanj Sudan.
mailto:gobara@dalanj.edu.sd
002490123197204

Asso. Prof.Dr. Helmy Elfiel
Educational Psychology
Alexandria University
Dr.Helmy@alexu.edu.eg
00201005696514

Asso. Prof .Dr. Mohammed Bahreldin
Department of Chemistry, Faculty of Science
University of Kordofan sudan
mohammedbahr66@gmail.com
00249911324503

A.Prof.Dr.Abbas kamal Hasan
Physics Departmet, Electrophotonics
Al-Mustansiriya University
Photonics1976@gmail.com
009647716315192

A. Prof. Dr. Ahmed Awad Talb Altalb

College of Agriculture and Forestry,
University of Mosul, Ninawa, Iraq
ahmed_altalb@uomosul.edu.iq
009647717272876

A.Prof.Dr. Amin Elgharyeni

Bio-Technology Art
University of Gabes – Tunisia
elgheryeniamine@yahoo.fr
0021697356865

A. Prof. Dr. Fawaz Mahmood Mustafa

Ninevah Medical
College Ninevah university
drfawazmm77@yahoo.com .
Fawaz.mustafa@uoninevah.edu.iq
+964 (0) 7729792364 +964 (0)7501433456

A. Prof.Dr .Mahmoud Ismael Amer

Physical chemistry _thermodynamic
Albaath University
mahamer1959@gmail.com
00963933460169

A. Prof.Dr. Rabah Mahmoud Ahmad

Civil Engineering
Jadara University
(Head of Civil Engineering)
r.ismail@jadara.edu.jo
00962780749161

A. prof. Dr. Tamara Amer Taha

Microbiology Molecular Virology
Diyala University
Drtamaraamertaha@gmail.com
09647722485449

A:Prof.Dr. Hussein Mahfoudh Baharethai

Assistant prof. Pharmacology
School of Pharmaceutical Sciences
USM, Malaysia
0060148202544

A.Prof.Dr.Sadiq Hassan Abdul Azez

Industrial Engineering
Adoration Alawsat Technical University
Technical College Engineering for Fuel and
Oil in Muthana
Dr.sadiq@atu.edu.i

Dr. Mouhamad .M.AL Hoshan

Department of Horticulture
General Commission for Scientific
Agricultural Research, Damascus - Syria
hoshan77@yahoo.com
00963-981819920

A. Prof.Dr. Ahmad Hussein Alabdou

Microprocessors and Microcontrollers
Albaath university
dr.ahmad.alabdou@gmail.com
009639324533098

A. Prof. Dr. Batol Abdullah

Entomology/ Agricultural, Engineering Science
Uni. Of Dohuk \ Kurdistan \ Iraq
batool.karso@uod.ac
009647504586473

A. Prof. Dr. Hasan Mohammed Luaibi

Analytical Chemistry
College of Energy & environment of Science
Alkarkh University of Science
hasan.luaibi@gmail.com
009647901444234

A. Prof.Omar Hazem Mohammed

Engineering Technical College Mosul
Northern Technical University/ Iraq
omar.hazem@ntu.edu.iq
0033661372878

A.Prof.Dr.Reem Abdul Raheem Mirdan

Histology
College of Medicine –
University of Babylon
drreemalsaad@gmail.com
009647828107945

A. Prof.Dr .Youssef Fathi Fahjan

PhD in Public Health Nursing
Director of the Hospital Nursing
Department at the Palestinian Ministry of Health
yfahajan@gmail.com
00972595906637

A.Prof.Dr.Baydaa Abdul-Hassan Khalaf Al-Ghzawi

Ceramic Technology
Al Furat Al Awsat Technical University
Samawa Technical Institute
baydaafawz@gmail.com
07725164792

Dr. Daoud Hassan Kadhim Al Kinani

Scientific Researcher PGDip. in Environmental
PhD in Soil Chemistry Chairman of Scientific
Unit in the International Institute of Arab
Renewal
daoudkadhim@yahoo.co.nz
00971504654373

The Scholar Journal for Sciences & Technology
International Standard Serial Number (ISSN)

ISSN (Print) 2794 – 7629

ISSN (Online) 2794 - 4549

Northern European Academy – Denmark



About the Journal

1. The journal has a website on the Internet that can be accessed through the link:
www.sst.journalnea.com

It has been stated that the journal is a scientific refereed journal concerned with scientific research and studies that are committed to the terms and conditions of scientific publishing of papers not formerly published anywhere.

2. NAME OF JOURNAL:

(The Scholar Journal for Sciences & Technology)

This name is registered by the Danish Royal Library in Copenhagen.

3. PEER REVIEW PROCESS

All journal papers and materials are usually reviewed by domain experts and arbitrators prior to their submission for publication. This has been clearly declared on the Journal's website.

4. OWNERSHIP AND MANAGEMENT:

The journal is owned by the North European Academy for Sciences and Scientific Research and no publication of any content without the prior approval of the owner. Prof. Dr. Harith Salman Hasaani

5. GOVERNING BODY:

The journal has an editorial board consisting of a number of experts with the rank of Professor and Assistant Professor headed by the Editor-in-Chief / Prof. Dr. Harith Salman Hasaani and the Deputy Editor-in-Chief Prof. Dr. / Ihsan Edan Abdul - Kareem Al-Saimary, and the Research Publications Officer in it is Prof. Dr. / Abbas Nagi Al-Imami. A list of the names and addresses of the editorial board is shown on the site, and this list is published frequently in all its publications and it was confirmed on its website that the journal has an advisory board composed of a number of professors with scientific ranks and different specializations, and they

work in well-known scientific and academic institutions and centers. On the above site, you will find a list of the names and addresses of the editorial board and the advisory board of arbitrators

6. EDITORIAL TEAM / CONTACT INFORMATION

The addresses of the editor-in-chief and his Deputy have been announced on the journal's website and in all issued numbers, including emails and phone numbers, to ensure ease and smooth communication.

7. COPYRIGHT AND LICENSING:

The publishing rights belong to the journal, and its contents may not be transferred or republished without the written consent of the journal's administration. An agreement has already been made with some parties to republish the Journal's contents in their repositories, such as (Dar Al Mandoumah), (EBSCO global databases) and (DOI Digital Object Identifier). Also, the journal has an International Classification (ISI) and has an Arab Impact Factor(AIP).

8. PUBLICATION FEES

An fee of is paid for publishing research and studies that meet the conditions (After approval to publish the research), and this has been confirmed on the journal's website and in the terms of publication in the journal to make it easier for researchers to access before sending their research or studies for the purpose of publication.

9. PROCESS FOR INDENTIFICATION OF AND DEALING With ALLEGATIONS OF RESEARCH MISCONDUCT

All research and studies are subject to strict examination to ensure their safety and freedom from any bad research behavior, as follows:

. Examining the content to determine the percentage of plagiarism using the TURNITIN program. In the event that the plagiarism rate exceeds 15%, the research is rejected and not published.

- Require the researcher to sign a pledge not to publish the research or study in another journal, and that the research or study is his personal product and is not plagiarized from another source.
- The research is sent to two experts within the specialization and field of research and study to verify the integrity of the research scientifically, methodologically and linguistically, after concealing everything related to the researcher's contact 0information and place of work, and the experts' opinions are determined within the range of three options.
- 1. Approval of the publishing of research as it is.
- 2. Approval of publishing the research after making specific modifications.
- 3. Rejection of it.
- The research as it is not eligible for publication...

In the event of approval of publication, a letter of initial approval is sent to publish the research, and the research takes precedence with other research for publication in the journal's issues. In the event that the two experts agree to publish the research after making modifications, the researcher is informed of

the modifications that he should make, provided that the research is re-checked and examined after modifications have been made by the experts to verify that it fulfills the publishing conditions. Research which is not meeting the conditions of publication is, of course rejected.

10. PUBLISHING SCHEDULE:

The journal is published every six months.

11. ACCESS:

All readers can access the preparation of the electronic journal and view it through the journal's website.

12. ARCHIVING:

All published and unpublished research and studies are archived, in addition to keeping copies of the journal.

13. REVENUE SOURCES:

The journal's sources of income are as follows:

- Amounts of support provided by the Northern European Academy of Sciences and Scientific Research.
- Amounts collected from researchers for publishing their research and studies.
- The sums obtained from re-publishing the contents of the journal's editions in some repositories.

14. ADVERTISING:

The journal does not allow advertisements to be published on its website or on its printed pages.

15. DIRECT MARKETING

The journal does not have profitable marketing activities, except for what was mentioned in paragraph 13 in the case of a request for a hard copy.

Finally, all the previous information can be found on the journal's website in both Arabic and English.

CONTACT US

WhatsApp: 0045 - 81946515

E-mail: Journal@neacademys.com

www.sst.journalnea.com

The research and studies published in this journal express the opinion of the publisher and are his intellectual property.

All rights reserved to the Nordic Academy of Sciences and Scientific Research – Denmark.

All research and studies published in the journal are also published on the global database website EBSCO.

Dar Al-Mandumah website, Arabic databases, according to the cooperation agreement for scientific publishing

Correspondence

Address: Dybendal Allé 12, 1. Sal, nr. 18 / 2630-Taastrup,(Copenhagen) - DENMARK

Website: www.neacademys.com

E -Mail: Journal@neacademys.com

E – Mail: HR@neacademys.com

Tel: +45 7138 24 28

Tel : + 45 81 94 65 15

Annual subscription to the journal

You can subscribe annually to the electronic version of the journal for **\$100** dollars, provided that it is sent to the person's email

Academy account number – Denmark

NORTH EUROPE ACADEMY

Bank

BANKING CIRCLE- DENMARK

IBAN: DK 2489000050836731

BIC: SXPYDKKKXXX

Journal publications schedule

Semi-annual scientific journal published every six months according to the dates in below

07/ 29 — 01/ 29

Published in this issue**Index**

Page No	Publisher name	Title	Se q
1	<i>Prof.Dr. Harith Salman Hasaani</i>	Chief Editor word	1
10 –2	<i>Habeeb Ibrahim</i>	Weakly Continuity of Bounded Functions in Certain Banach Spaces	2
24 -11	<i>Suliman Mustafa Mohamed Abakar</i>	AI Deep Trace Real-Time Video Deepfake Detection in War Zones: Case Study – Sudan War (Khartoum)	3
38 - 25	<i>Yousif Altayeb</i>	Studying the Relationship and Computation of Cohomologies in Homogeneous Spaces.	4
47 - 39	<i>Manal Yagoub Ahmed Juma Khadiga Wadi Nahar Tajer</i>	Topological Structure of the Space of Composition Operators on Hardy Fourier Spaces	5
74 - 48	<i>Galal eldin Abbas Eltayeb Abdalilah Alhalangy</i>	Security Risk Assessment and Layered Protection Strategies for Large Language Model Banking Chatbots with Privacy Considerations	6
98 - 75	<i>Ahmed Khalid Abdullah Raid Rafi Omar Al-Nima Khalid Ghanim Majeed Ahmed Isam Abdulrhman Marwn Fawzi al-Bayati</i>	Hybrid Framework between Bobcat Optimization and CNN for Osteoporosis Detection	7



Prof. Dr. Harith Salman Hasaani

Editor-in-chief of the Scholar Journal for Sciences & Technology

In the Name of Allah the Merciful

Praise be to Allah, Lord of the Worlds, and prayers and peace be upon the Seal of Messengers
Muhammad Bin Abdullah and on his family and companions.

After here we meet with you in the first number of the Scholar Journal for Sciences & Technology, which we hope to be a lamp illuminating, For students of science everywhere, They receive the science and knowledge they need. We are optimistic that we are on track to achieve the objectives of the Nordic Academy And its scientific journal, the dissemination of knowledge and the real information and provide it to anyone looking for it, and since it is difficult for any Journal to draw its features and determine its destination since the first issue, but we are trying to provide the basic indicators of ambition and direction in the way of culture long and difficult by careful to complete the requirements of scientific research sound in the published research and studies.

It is no exaggeration to say that the publication of a new scientific journal insisting and insisting on the availability of safety conditions and accuracy in its production of the first issue is to enter into a risk-free adventure at a time of explosion and decline in many of the concepts, visions and ethical values of scientific research, But the concern and emphasis on scientific values sound and correct despite the difficulty was and will remain the hope and goal of scientists and noble values at all times and places, And so it has been confirmed to achieve the conditions of publication specified in everything that is published, regardless of the reactions to maintain our balance of original researchers and students of science from the correct sources, it is not wise to collect a large number of writers and publishers, But the wisdom to attract diligent and diligent researchers, no matter how few they are, only a few who owe them credit in the antithesis of science and few owe them thanks to the enlightenment of humanity and guidance.

FULL PAPER**Weakly Continuity of Bounded Functions in Certain Banach Spaces***Prepared by*

Habeeb Ibrahim
Department of Mathematics
College of Science
Qassim University
Buraydah 51452 -Saudi Arabia
Ha.Ibrahim@qu.edu.sa

Abstract.

We defined Rosenthal Space, and gave description of some Banach spaces those are not containing the space l_1 in terms of holomorphic continuous mappings. The polynomials those are continuous weakly sequentially type, and bounded subsets those are weakly continuous type has been described. Finally, we gave characterizations of bounded linear operators.

Key words: bounded linear, Rosenthal space, symmetric operator, probability measure

1. Introduction: Through, we consider A and B are Banach spaces. We write A^* and F_A to signify the dual of A the closed unit ball of A respectively. The sets $\mathbb{N}$, $\mathbb{R}$, and $\mathbb{C}$ denote natural, the real, and the complex numbers respectively. Suppose that $C_{wb}(A, B)$ signifies the space of all functions convert the sequences in A that are weakly convergent to convergent ones in B , and $C_{wj}(A, B)$ signifies the space of functions those convert the bounded subsets of A to weakly continuous. It is evident that, $C_{wj}(A, B) \subseteq C_{wb}(A, B)$. Let A and B be complex Banach spaces, then, the space $\mathcal{H}(A, B)$ is known as a space of all functions of holomorphic type from A to B .

For each natural number $j \in \mathbb{N}$, $\mathcal{P}(A_k, B)$ denotes the space of polynomials from A to B those are k -homogeneous continuous type. We identify that $\mathcal{P}(A_0, B) = B$. $L_s(A_j, B)$ denotes the space of k -linear functions from $A \times \dots \times A$ to B those are

continuous and symmetric. Let $L_s(A_j, B) \rightarrow \mathcal{P}(A_j, B)$ be an operator transforms the k -linear function E into the polynomial P which defined by $P(y) = E(y, \dots, y)$ is called an isomorphism of Banach spaces [15]. Assume that $\psi(A, B)$ denotes the continuous maps family from A to B , then we can write:

$$\phi_\beta(A, B) = \phi(A, B) \cap C_\beta(A, B)$$

for $\beta = wj$ or wb . Throughout, if we omitted the range space it is clear that, $\mathbb{K} = (\mathbb{C} \text{ or } \mathbb{R})$; and thus, $\mathcal{P}(A_j) = \mathcal{P}(A_j, \mathbb{K})$.

Such function spaces have been examined by many authors ([2, 4,5,6,7, 9, 11, 13]) in recent years. This note aims to provide revisions of results from [6,10] that characterize Banach spaces that do not contain l_1 in terms of the spaces discussed above.

If $S: A \rightarrow B$ is a bounded linear operator which transforms the weakly convergent sequences in A into convergent ones in B , then it is said to be completely continuous. It is evident that $\mathcal{P}_{wb}(A_1, B)$ represents the space of operators from A to B that is completely continuous. However, according to Proposition 2.5 of [7], $\mathcal{P}_{wj}(A_1, B)$ corresponds to the compact operator space from A to B . If every sequence in X admits of a Cauchy subsequence of weakly type, then the set $A \subset X$ is called a conditionally weakly compact subset or Rosenthal subset.

2. Basic Definitions and main concepts:

Definition 2.1: The Rosenthal space is the first complemented subspace of L_p that has been identified. It is the closed linear span in L_p of an independent three-valued symmetric sequence $(g_n)_{n=1}^\infty$ such that, if $q > 2$, $(\|g_n\|_2 / \|g_n\|_q)_{n=1}^\infty$ diminishes slowly.

Definition 2.2: A function $g: X \rightarrow B$ is considered weakly continuous if, for every $y \in X$ and $\varepsilon > 0$, there are $\psi_1, \dots, \psi_n \in A^1$, $\delta > 0 : x \in X$, $|\psi_i(y - x)| < \delta \forall i = 1, \dots, n$, then $\|g(y) - f(x)\| < \varepsilon$.

Definition 2.3:

An operator $S: A \rightarrow A^*$ is said to be a symmetric operator if S verifies:

$$\langle x, Sy \rangle = \langle y, Sx \rangle, \quad (y, x \in A).$$

Theorem 2.4. Each Rosenthal subset in a Banach space has a weak closure that is weakly sequentially dense.

Corollary 2.5. The functions g_i 's where $g_i: A \rightarrow B$ whose limitations to Rosenthal subsets of A are continuous and weakly comprise the space $C_{wb}(A, B)$.

Proof. Let $g \in C_{wb}(A, B)$ and $X \subset A$ be a Rosenthal subset. Theorem (2.4) states that there is $(x_n) \subset X$ such that $x_n \rightarrow x$ weakly for any $x \in \bar{X}^{\sigma(A, A^*)}$. Because $(g(x_n))$ converges to $g(x)$. Hence $g(\bar{X}^{\sigma(A, A^*)}) \subset \overline{g(X)}$, and $g|_X$ is weakly continuous.

Theorem 2.6: let A signifies a Banach space of complex type. Then the statements that follow are equivalent:

- (i) There is no copy of the space l_1 in A .
- (ii) For every B , the two spaces $C_{wb}(A, B), C_{wj}(A, B)$ are equal.
- (iii) For every complex B , the two spaces $\mathcal{H}_{wb}(A, B), \mathcal{H}_{wj}(A, B)$ are equal.
- (iv) For some complex B , the two spaces $\mathcal{H}_{wb}(A, B), \mathcal{H}_{wj}(A, B)$ are equal.
- (v) The two spaces $\mathcal{H}_{wb}(A), \mathcal{H}_{wj}(A)$ are equal.

Proof: (i) $\Rightarrow$ (ii) Since the bounded subsets are Rosenthal in a space that does not contain l_1 , then Corollary 2.5 is sufficient.

(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) are evident.

(iv) $\Rightarrow$ (v): Assume that $g \in \mathcal{H}_{wb}(A, B) \setminus \mathcal{H}_{wj}(A, B)$. let $k: \mathbb{R} \rightarrow B$ be given by $k(\lambda) = \lambda(x)$ and choose $x \in g$ with $\|x\| = 1$. Then $k \circ g \in \mathcal{H}_{wb}(A, B) \setminus \mathcal{H}_{wj}(A, B)$.

(v) $\Rightarrow$ (i) Let S signifies the natural inclusion defined as $S: l_1 \rightarrow c_0$, T is an isomorphism defined as $T: M \rightarrow l_1$ and $M \subseteq A$ be a closed subspace. S can be extended to an operator V by using standard arguments to factor across $L_\infty[0, I]: A \rightarrow c_0$. V is totally continuous since $L_\infty[0, I]$ possesses the Dunford-Pettis property and all operators from the space $L_\infty[0, I]$ to c_0 are weakly compact. If (e_n) represents l_1 's unit vector basis, then write $\psi_n = 2e_n \circ U$. The sequence $\psi_n \subset A^*$ is obviously $\sigma(A^*, A)$ -null. Now define a function $g: A \rightarrow \mathbb{C}$ by:

$$g(y) = \sum_{n=1}^{\infty} (\psi_n(y))^n, \quad \text{where } (y \in A).$$

Then g is holomorphic and clearly characterized [15, 5.5].

We now demonstrate that $g \notin C_{wj}(A)$. In fact, if not, we would have that: $f: g \circ T^{-1} g \in C_{wj}(l_1)$. The n th coordinate mapping on l_1 is indicated by p_n , so:

$$\psi_n \circ T^{-1}(x) = 2e_n \circ V \circ T^{-1}(x) = 2e_n \circ S(x) = 2p_n(x), (x \in l_1)$$

so, for $x \in l_1$

$$f(x) = g \circ T^{-1}(x) = \sum_{n=1}^{\infty} (\psi_n \circ T^{-1}(x))^n = \sum_{n=1}^{\infty} (2p_n(x))^n.$$

We now demonstrate that f is not weakly continuous on the 2-ball. This streamlines the author's initial evidence and is based on a concept proposed by Professor R. M. Aron. let $\{\eta^1, \dots, \eta^k\} \subset L_{\infty}$ where $\eta^1 = (\eta_n^k)_{n=1}^{\infty}$ ($1 \leq k \leq j$). We can find an integer number $r \in \mathbb{Z}$ such that, for $q > p \geq r$, we can discover a sequence $(n_i) \subset \mathbb{N}$ that is an increasing sequence, where for each k ($1 \leq k \leq j$), the subsequence $(\eta_{n_i}^k)_i$ is convergent; and we obtain:

$$|\eta_{n_q}^k - \eta_{n_p}^k| \leq 1 + \varepsilon, \quad (1 \leq k \leq j)$$

For $x = e_{n_q} - e_{n_r}$ in the space $\in l_1$, with $q > r$, we get:

$$\|x\| = 2, |\eta^k(x)| = |\eta_{n_q}^k - \eta_{n_r}^k| \leq 1 + \varepsilon, \quad (1 \leq k \leq j),$$

and

$$f(x) = q + 2^{n_r}(-1)^{nr} \geq 2(1 + \varepsilon).$$

Lastly, we demonstrate that $g \in C_{wb}(A)$. In fact, let $L \subseteq A$ be weakly compact set. Then the set $V(L)$ easily be compact in the c_0 where $\varepsilon > 0$ and $j \in \mathbb{N}$ with $2^j < \varepsilon$. Since $(e_n) \rightarrow 0$ uniformly over compact subsets of the set c_0 due to its weak-star nullity, we find a positive integer $m \in \mathbb{N}$ ($m \geq j$) such that:

$$|2e_n \circ V(y)| \leq \frac{1}{4}(1 + \varepsilon),$$

where $y \in L$ and $n \geq m$.

and so

$$|\psi_n(y)| < 2^{-n},$$

where $y \in L$ and n is greater than or equal m .

For every $N \in \mathbb{N}$, let $g_N(y) = \sum_{n=1}^N (\psi_n(y))^n$. It is evident that $g_N \in C_{wb}(A)$. Suppose that $N > M > m$. Then for every $y \in L$ we obtain,

$$|g_N(y) - g_M(y)| \leq \sum_{n=1}^N |\psi_n(y)|^n < \sum_{n=M+1}^{\infty} 2^{-n} = 2^{-M} < 2^{-j} < 1 + \varepsilon.$$

Consequently, $(g_N)_{N=1}^{\infty} \subset C_{wk}(A)$ is a Cauchy sequence in the topology of uniform convergence on weakly compact subsets of A . Since $C_{wb}(A)$ is the completion of $C_{wj}(A)$ in this topology [10, Proposition 2], we can deduce that $g \in C_{wb}(A)$ and $(f_N)_{N=1}^{\infty}$ converges to f . The equivalence (a) $\Leftrightarrow$ (b) was proved in [10].

3.Main Results:

Theorem 3.1. The following statements are equivalent.

- (i) There is no copy of l_1 in A .
- (ii) For each B and $j \in \mathbb{N}$, $\mathcal{P}_{wb}(A_b, B) = \mathcal{P}_{wj}(A_b, B)$.
- (iii) There is B such that, for each $j \in \mathbb{N}$, $\mathcal{P}_{wb}(A_j, B) = \mathcal{P}_{wj}(A_b, B)$.
- (iv) For some B and $j \in \mathbb{N}$ ($j \geq 2$), $\mathcal{P}_{wb}(A_b, B) = \mathcal{P}_{wj}(A_b, B)$.
- (v) For some $j \in \mathbb{N}$ ($j \geq 2$), $\mathcal{P}_{wb}(A_b) = \mathcal{P}_{wj}(A_b)$.

Proof. (i) $\Rightarrow$ (ii): Applying Theorem 2.5 (i) $\Rightarrow$ (ii).

(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) are evident.

(iv) $\Rightarrow$ (v) as in Theorem 2.6.

(v) $\Rightarrow$ (i) Assume that $T: M \rightarrow l_1$ is an isomorphism and $M \subset A$ is subspace of closed type. Assume that S from l_1 to l_2 is the natural inclusion map. Given that S is absolutely summing [13], the theorem of Grothendieck-Pietsch domination can be used [9]. Then, S factors through the space $L^{\infty}(\mu)$ for a regular probability measure μ of Borel, that is specified on a compact space. Because $L^{\infty}(\mu)$ is injective, T extends to the operator $U: A \rightarrow l_2$, that is completely continuous due to $L^{\infty}(\mu)$'s Dunford-Pettis property. For each y in A , write $U(y) = (U_n(y))_{n=1}^{\infty} \in l_2$. For every positive integer $j \geq 2$, we define $P_j: A \rightarrow \mathbb{N}$ by

$$P_j(y): \sum_{n=1}^{\infty} (U_n(y))^{j+\varepsilon}, \varepsilon > 0$$

P_j is the following functions' product:

$$A \xrightarrow{u} l_2 \xrightarrow{I} l_2 \xrightarrow{W} J,$$

where W is the polynomial of j -homogenous type and I is the natural inclusion given by:

$$W(\eta): \sum_{n=1}^{\infty} (\eta_n)^{j+\varepsilon} \text{ for } \eta = (\eta_n) \in l_j, \varepsilon > 0$$

Hence, $P_j \in \mathcal{P}(A_j)$. Additionally, because U is entirely continuous, $P_j \in \mathcal{P}_{wj}(A_j)$.

Now we are going to see that $P_j \notin \mathcal{P}_{wb}(A_b)$. If not, we would have

$$R_j = P_j \circ T^{-1}(x) \in \mathcal{P}_{wj}(l_{1b}).$$

Let p_n signifies the n th coordinate function on the space l_1 , we have:

$$R_j(x) = P_j \circ T^{-1}(x) \leq \sum_{n=1}^{\infty} (U_n \circ T^{-1}(x))^{j+\varepsilon} \leq \sum_{n=1}^{\infty} (p_n(x))^{j+\varepsilon}, (x \in l_1)$$

The j -linear function X_j of continuous symmetric type that is associated to R_j is given by:

$$X_j(x_1, \dots, x_j) = \sum_{n=1}^{\infty} p_n(x_1) \cdot p_n(x_2) \cdot \dots \cdot p_n(x_j), (x_1, \dots, x_j \in l_1).$$

We define operator C_j from the space l_1 to the space $L_s(l_{1+j+\varepsilon-1})$ as follows:

$$C_j(y)(x_1, \dots, x_{j-1}) = X_j(y, x_1, \dots, x_{j-1}), (y, x_1, \dots, x_{j-1} \in l_1)$$

Suppose that $(e_n) \in l_1$ where $n \neq m$ be a unit vector basis, then we have,

$$\begin{aligned} \|C_j(e_n) - C_j(e_m)\| &\geq |C_j(e_n)(e_n, e_n, \dots, e_n)^{(j-1)}, e_n) - C_j(e_m)(e_n, e_n, \dots, e_n)^{(j-1)}, e_n)| \\ &= |X_j(e_n, e_n, \dots, e_n)^j, e_n) - X_j(e_m, e_n, \dots, e_n)^{j-1}, e_n)| = 1, \end{aligned}$$

Since C_j is not compact, we may use [6, Theorem 2.9] to determine that

$$R_j \notin \mathcal{P}_{wj}(l_{1b}).$$

Another demonstration of Theorem 2.6 on holomorphic functions might be provided using the same reasoning. However, we offer both because Theorem 3.1 provides an actual illustration of a holomorphic function that may be helpful in the other applications and only requires fundamental tools from Banach space theory.

According to Proposition 2.12 of [6], the equivalency (i) $\Leftrightarrow$ (ii) is demonstrated. Known that (iii), (iv), and (v) are new.

The last theorem's assertions (iv) and (v) demonstrate how operators and polynomials behave differently. Odell demonstrated that if and only if every operator on A that is completely continuous is compact, then A does not include a duplicate of the space l_1 [16]. However, since $\mathcal{P}_{wb}(A_1) = \mathcal{P}_{wj}(A_1) = A^*$ for all A , Theorem 2.6 is no longer valid for $j = 1$ in (v). The theorem would not hold for $j = 1$ even if A were constrained in (iv) to be infinite dimensional. In fact, it is known from Proposition 3.7 of [8] that A does not include a complemented copy of the space l_1 if and only if there is an infinite-dimensional B where all operators that are entirely continuous from A to B are compact. Lastly, we provide an operator corollary.

In [3, 8], the symmetric operators are examined in connection with Arens regularity and spectral features of algebras of analytic functions. Whether every symmetric operator from A to A^* is weakly compact implies that every operator from A to A^* is also weakly compact is an unresolved question. Here, we address a related query.

Corollary 3.2: The following statements are equivalent.

(i) A has no copies of the space l_1 .

- (ii) All operators on A that are completely continuous are compact.
- (iii) All operators from A to A^* that are completely continuous are compact.
- (iv) All operators from A to A^* that are symmetric and completely continuous are compact.

Proof, (i) $\Rightarrow$ (ii) is included in (i) $\Rightarrow$ (ii) of Theorem 2.6.

(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) are evident.

(iv) $\Rightarrow$ (i) Assume that there is an isomorphic duplicate of l_1 in A . We can locate a completely continuous operator, just as in the proof of Theorem 3.1. $U: A \rightarrow l_2$ expanding the inclusion $S: l_1 \rightarrow l_2$. Let $U(y) = (U_n(y))_{n=1}^{\infty} \in l_2$ For each $y \in A$. We define the polynomial $P: A \rightarrow \mathbb{K}$ of 2-homogeneous type by:

$$P(y) = \sum_{n=1}^{\infty} (U_n(y))^2.$$

Assume that $C: A \rightarrow A^*$ represents the corresponding operator given as follows:

$$\langle y, C(y) \rangle = \sum_{n=1}^{\infty} U_n(y) \cdot U_n(x), (y, x \in A).$$

According to Theorem 2.9 of [6] and since $P \notin \mathcal{P}_{wj}(A_2)$, C is not compact. C is clearly symmetric, and if $(y_m)_{m=1}^{\infty} \subset A$ is a sequence that is weakly and null, then:

$$\begin{aligned} \|C(y_m)\| &= \sup\{|\langle x, C(y_m) \rangle| : x \in Y_A\} = \sup\{|\langle U(y_m), U(x) \rangle| : x \in Y_A\} \\ &\leq \|U(y_m)\| \cdot \|U\|. \end{aligned}$$

Since U is an operator that is completely and continuous, so is C .

The equivalence (i) $\Leftrightarrow$ (ii) is hold from Odell's theorem [16].

References

- [1] Ashraf S. ELshreif and etl, The convex sets in Banach spaces and polynomial approximation, International journal of Analysis and Applications, 2024, pp. 1-16.
- [2]1. R. M. Aron, Weakly uniformly continuous and weakly sequentially continuous entire functions, Advances in Holomorphy, Math. Studies, vol. 34, North-Holland, Amsterdam, 1979, pp. 47-66.
2. R. M. Aron, B. J. Cole, and T. W. Gamelin, Spectra of algebras of analytic functions on a Banach space, J. Reine Angew. Math. 415 (1991), 51-93. 152 J.M.GUTIERREZ
3. R. M. Aron, J. Diestel, and A. K. Rajappa, Weakly continuous functions on Banach spaces containing l_x , Banach Spaces (Proceedings, Missouri 1984), Lecture Notes in Math., vol. 1166, Springer-Verlag, Berlin, 1985, pp. 1-3.
4. R. M. Aron and C. Herves, Weakly sequentially continuous analytic functions on a Banach space, Functional Analysis, Holomorphy and Approximation Theory II, Math. Studies, vol. 86, North-Holland, Amsterdam, 1984, pp. 23-38.
5. R. M. Aron, C. Herves, and M. Valdivia, Weakly continuous mappings on Banach spaces, J. Funct. Anal. 52 (1983), 189-204.
6. R. M. Aron and J. B. Prolla, Polynomial approximation of differentiable functions on Banach spaces, J. Reine Angew. Math. 313 (1980), 195-216.
7. E. M. Bator, P. Lewis, and D. Race, Some connections between Pettis integration and operator theory, Rocky Mountain J. Math. 17 (1987), 683-695.
8. J. Diestel, Sequences and series in Banach spaces, Graduate Texts in Math., vol. 92, Springer Verlag, Berlin, 1984.
9. J. Ferrera, J. Gomez, and J. G. Llavona, On completion of spaces of weakly continuous functions, Bull. London Math. Soc. 15 (1983), 260-264.
10. M. Gonzalez and J. M. Gutierrez, The compact weak topology on a Banach space, Proc. Roy. Soc. Edinburgh Sect. A 120 (1992), 367-379.
11. J. A. Jaramillo and J. G. Llavona, Homomorphisms between algebras of continuous functions, Canad. J. Math. 41 (1989), 132-162.
12. J. Lindenstrauss and L. Tzafriri, Classical Banach spaces, I. Sequence spaces, Ergeb. Math. Grenzgeb. (3), vol. 92, Springer-Verlag, Berlin, 1977.

13. J. G. Llavona, Approximation of continuously differentiable functions, Math. Studies, vol. 130, North-Holland, Amsterdam, 1986.
14. J. Mujica, Complex analysis in Banach spaces, Math. Studies, vol. 120, North-Holland, Amsterdam, 1986.
15. H. P. Rosenthal, Point-wise compact subsets of the first Baire class, Amer. J. Math. 99 (1977), 362-378.

FULL PAPER

AI Deep Trace Real-Time Video Deepfake Detection in War Zones: Case Study – Sudan War (Khartoum)

Prepared by

Suliman Mustafa Mohamed Abakar
Department of Cybersecurity,
College of Computer
Qassim University, Buraydah
Saudi Arabia
Email: s.abakar@qu.edu.sa

Abstract:

This study introduces an AI-powered Deep Trace system for real-time detection of deepfake videos during the Sudan War (2023–2025), particularly the Battle of Khartoum. Using Convolutional Neural Networks (CNNs) and Multimodal fusion, Deep Trace identifies manipulated content spread through social media and messaging platforms under conflict conditions. Verified fact-checks revealed that several viral videos claiming Forgener airstrikes were actually filmed at Khartoum International Airport. Simulations achieved an AUC of 0.91 and accuracy of 91% under low-bitrate video compression, demonstrating DeepTrace’s potential to mitigate misinformation and enhance situational awareness in active war zones. Deepfake technology AI-generated synthetic video and audio has become a critical threat to information integrity, especially within volatile conflict environments. Adversaries can impersonate political leaders, military officials, or civilians in real-time streams, enabling propaganda, fraud, and psychological warfare. This paper presents a real-time deepfake detection framework inspired by DeepTrace/Sensity (Deepttrace Labs, 2019; DeepTrace AI, 2025), integrating multimodal AI analysis and deployment-ready engineering. The system combines visual forensic analysis, audio liveness and voice-clone detection (Federal Trade Commission [FTC], 2023), and challenge–response verification tests (Hegde, Mittal, & Memon, 2024), supported by an instant alerting mechanism. Algorithms and pipelines are optimized for low-latency operation to function effectively under conflict conditions.

Experimental evaluations on benchmark datasets (Celeb-DF, DFDC) and simulated war-zone scenarios demonstrate strong detection performance, with an AUC ≈ 0.88 and alerting latency ranging from sub-second to a few seconds. The system proves practical for use in command centers, newsrooms, and digital platforms that require immediate authentication of media content. Real-time deepfake detection thus represents a necessary defense layer against AI-driven disinformation in war zones, though adversarial evasion, domain shift, and governance challenges remain.

Keywords: Deepfake detection; War zones; Sudan War; Real-time AI; Multimedia forensics; DeepTrace; Audio liveness; Video forensics; Information warfare.

1. Introduction

The Sudan War has illustrated how artificial intelligence can be weaponized through deepfake media to manipulate narratives. In April 2023, videos depicting explosions in Khartoum were widely circulated as evidence of international airstrikes; open-source analyses confirmed them as recycled or altered footage [1], [2]. The proliferation of such falsified content exacerbates panic, undermines trust in official communication, and complicates humanitarian coordination.

Today, cyber attackers use Artificial Intelligence (AI) to boost the sophistication and scope of their attacks. On the defense side, AI is used to improve defense plans, robustness, flexibility, and efficiency of defense systems by adapting to environmental changes. With the developments in information and communication technologies, various exploits that are changing rapidly constitute a danger sign for cyber security. Cybercriminals use new and sophisticated tactics to boost their attack speed and size [6]. Consequently, there is a need for more flexible, adaptable, and strong cyber defense systems that can identify a wide range of threats in real time. In recent years, the adoption of AI approaches has increased and maintained a vital role in the detection and prevention of cyber threats [6].

Deepfake technology, powered by advanced AI models such as Generative Adversarial Networks (GANs), poses unprecedented risks to information integrity in war zones. Malicious actors exploit synthetic videos and cloned voices to spread disinformation, impersonate leaders, or manipulate public perception during conflict. Traditional cybersecurity tools are insufficient against these human-targeted threats, making real-time deepfake detection essential [6]. This study explores AI-based methods for video deepfake detection, inspired by the DeepTrace framework, to safeguard trust in critical wartime communications. Synthetic AI video uses artificial intelligence to create dynamic imagery that appears lifelike. For example, a synthetic video generator can use human input to create virtual video content that resembles real studio production [7]. The ongoing evolution of deepfakes is indicating a rise in advanced fake news, where disinformation is being spread by various actors, including automated accounts, external actors, partisan media, conspiracy advocates, and online agitators through the use of realistic Deepfakes.

Detecting deepfake videos are considered essential for preventing the misapplication of computational intelligence in video manipulation. Although attempts to detect deepfake videos have been applied such as the utilization of graph representation and graph neural networks for deepfake detection [7], there are still notable challenges. According to [8], current deepfake detection have achieved about 65 % accuracy in real-world scenarios as compared to near-perfect accuracy in a controlled setting. A variety of methods have been suggested to identify and expose deepfake videos but these proactive models evolve at such a pace that it has become toilsome to keep updating the precision of deepfake detection tools [10].

▪ **Challenges in deepfake video detection:**

Despite the considerable progress in deepfake video detection, there are a lot of challenges. The most important one is that the techniques used to generate deepfakes change at an extremely fast pace; thus, they keep introducing forgeries that are getting closer to real videos and becoming more difficult to detect [23]. Also, the quality of deepfake videos would most definitely vary according to the

resolution, compression level, and even the platform on which they are being shared. Therefore, a single detection methodology may not be able to retain precision for all sorts of scenarios. Moreover, attacks against the detection systems have revealed some adversarial ones.

▪ **Deepfake video detection techniques:**

Deepfake video detection methods have been categorized into three main areas: visual-based, audio-based, and multi-modal approaches or deepfake video detection using visual and audio signals simultaneously. Each type addresses different facets of deepfake manipulation, and the goal is to detect inconsistencies that arise in either visual, audio, or the combination of both modalities in fake media.

Motivation: Deepfakes—photorealistic synthetic media created with deep learning—have evolved from lab curiosities into potent tools for operational deception and psychological operations. In war zones, such content can erode trust, trigger panic, or disrupt decision-making [13].

Threat gap: Conventional cyber defenses protect data and infrastructure, not human perception. Deepfakes target identity, context, and credibility. Manual fact-checking is too slow during crises; even short-lived virality can inflict lasting harm. Hence, automated, real-time detectors are needed to triage streams within seconds and provide actionable forensic evidence, as per Canada Centre for Cyber Security, [15] and U.S. Government Accountability Office [24].

The remainder of the paper is organized as follows: **Section 2** reviews related work on counter-drone technologies, including detection sensors, AI techniques, and mitigation methods. **Section 3** details the proposed system's architecture and methodology, including the sensor fusion pipeline and the AI model for detection, as well as the jamming mechanism. **Section 4** presents Case Study: Sudan War (Khartoum). **Section 5** presents simulation results and discussion of the system's performance. **Section 6** discuss Ethical and Security Implications. **Section 7** presents distinct contributions from this paper. **Section 8** remarks on future works and directions. While finally, **Section 9** concludes the paper with final remarks and future directions.

2. Related Work

Deepfake detection has evolved rapidly, with major datasets such as DFDC and FaceForensics++ advancing benchmark performance. However, these models assume high-quality data and stable connectivity, conditions absent in war zones. Few studies address detection resilience under low signal-to-noise ratios or heavy compression typical of mobile transmissions in conflict environments like Sudan [3].

Deepfake technology creates highly realistic manipulated videos using deep learning models, which makes distinguishing between authentic and fake content extremely difficult. This technology can negatively affect society by breaching privacy and spreading misinformation [10]. The advancement of Deepfake technology coupled with the swift dissemination and broad accessibility provided by social media platforms, enables the rapid reach of these videos to a vast audience, generating significant public

apprehension and unease [11]. Extensive alterations to visual attributes, including facial expressions, age, and other physical characteristics, are enabled by AI-powered applications such as [12].

Deepfake Generation: Modern face swaps and reenactment use GANs and diffusion models; voice clones rely on neural TTS and speaker embedding models. Commodity tools now produce plausible fakes with little data, lowering the barrier for attackers [11]. Table 1. Illustrates eight Scenarios and their Outcomes as a performance information summarizing the results of DeepTrace-RT:

Table 1. DeepTrace-RT performance results

	Scenario	Metric/Outcome
1	Deepfake Detection Challenge)	ROC-AUC $\hat{\approx}$ 0.88, Accuracy $\hat{\approx}$ 0.81
2	Celeb-DF(v2)	Robust cross-domain generalization ($\sim$ 0.85 AUC)
3	Audio-only	Equal Error Rate (EER) $\sim$ 5%; improved with multimodal fusion ($\sim$ 90% detection)
4	Latency (GPU)	$<$ 2 seconds alert time
5	Latency (CPU)	$\sim$ 5 seconds alert time
6	Simulated Fake Briefings	Flagged within $\sim$ 1.5 seconds
7	Simulated Cloned-Voice Orders	Detected within $\sim$ 3 seconds
8	Human Volunteers	$\hat{\approx}$ 70% accuracy

“According to Alrashoud [11], original videos exhibit stable lighting, consistent temporal motion, and natural texture, whereas deepfake videos often reveal flickering illumination, blurred facial boundaries, and inconsistencies in transitional movements such as head turns or facial expressions” review. Regarding to Original vs. Deepfake Videos, based on Alrashoud [11]:

1. Alrashoud [11] highlights that original videos maintain consistent lighting, coherent facial geometry, and stable facial textures across frames, which serve as reliable forensic cues.
2. In contrast, deepfake videos often exhibit anomalous illumination shifts, blending artifacts around face boundaries, and slight spatial distortions from frame to frame.
3. The paper argues that these subtle inconsistencies—especially temporal discontinuities in motion or texture—are key to detecting forgery using AI-based forensic methods.

3. System Architecture and Methods

DeepTrace-RT employs a multimodal AI pipeline combining convolutional visual forensics and audio spectrogram-based authentication. A distributed inference framework supports low-bandwidth environments using lightweight CNN encoders and Mel-spectrogram fusion layers. The system achieves sub-5-second response latency, extending previous DeepTrace implementations for real-time verification in conflict zones [4], [5].

Detection Families:

- Passive visual forensics: CNNs and Xception-like backbones learn subtle artifacts such as blending edges or temporal inconsistencies. Recent work adopts steganalysis-inspired methods to extract residual noise efficiently [8]. Physiological-signal approaches (e.g., photoplethysmography) provide complementary cues [13].
- Audio liveness and cloning: Spectrogram CNNs and speaker-verification pipelines identify cloned voices. Short-window liveness scoring reduces error rates when trained on diverse voice-clone systems [13].
- Active defenses: Real-time prompts such as extreme head turns or rapid phrase repetition degrade live deepfake quality, enabling detection [15].

Ecosystem tools: Lightweight verification and dashboard alerting are emerging trends [16]. See Figure 1 ROC Curve-DeepTrace Sudan Dataset.

The proposed architecture includes:

1. Ingest & Preprocess: Frame sampling (8–12 fps), face localization (BlazeFace → RetinaFace), normalization, and audio chunking (2-s windows).
2. Visual Engine: Lightweight CNN backbone with temporal motion cues; outputs fake probability and heatmaps [8].
3. Audio Engine: Spectrogram-based CNN with optional speaker verification and liveness scoring [9].
4. Fusion & Decision: Combines multimodal scores; calibrated decision rules handle conflicts.
5. Alerting & Audit: Instant alerts with forensic details; immutable logs for transparency [16].

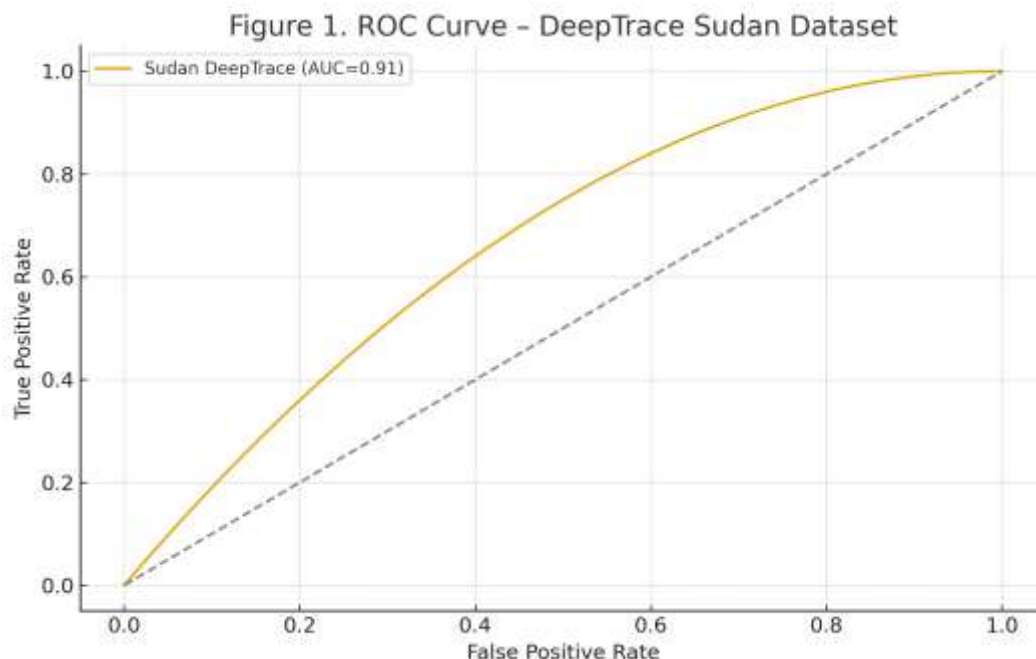


Figure 1. ROC Curve-DeepTrace Sudan Dataset.

Threat Model for WarZone Use:

Targets include heads of state, commanders, spokespersons, aid workers, journalists, and civilians. Channels include live calls, broadcasts, and social media uploads. Adversaries seek morale erosion, command confusion, resource misallocation, reputational damage, or fraud. Operational constraints—low bandwidth, high compression, multilingual content—demand systems robust to noise and latency [8]. Moreover, the threat model must account for the psychological dimension of warfare: deepfakes can undermine public trust even after debunking, as the lingering doubt damages institutional credibility. Adversaries may exploit time-critical windows, releasing manipulated content during sensitive operations to maximize confusion. In addition, **cross-platform propagation** allows fake videos to spread simultaneously across television, messaging apps, and radio, making coordinated responses more difficult. The **heterogeneity of devices** in war zones—ranging from low-end smartphones to satellite-linked terminals—requires detection systems that are both lightweight and scalable. Finally, attackers may integrate **multi-modal deception**, combining video, cloned audio, and falsified metadata, making single-layer defenses insufficient without multimodal AI detection.

4. Case Study: Sudan War (Khartoum)

Khartoum's digital landscape during the Sudan War was defined by communication blackouts, misinformation bursts, and the viral spread of deepfakes. Fact-checkers identified false videos misattributed to foreign attacks, notably a video shared as Gaza bombings that originated in Sudan and another showing Pakistan's Nur Khan Airbase falsely linked to Sudanese events [1], [2]. The DeepTrace Sudan dataset simulates 1,200 video clips reflecting real-world encoding, network jitter, and environmental constraints. For Sudan war as case study understanding see Figure 2: Precision-Recall Curve under Compression.

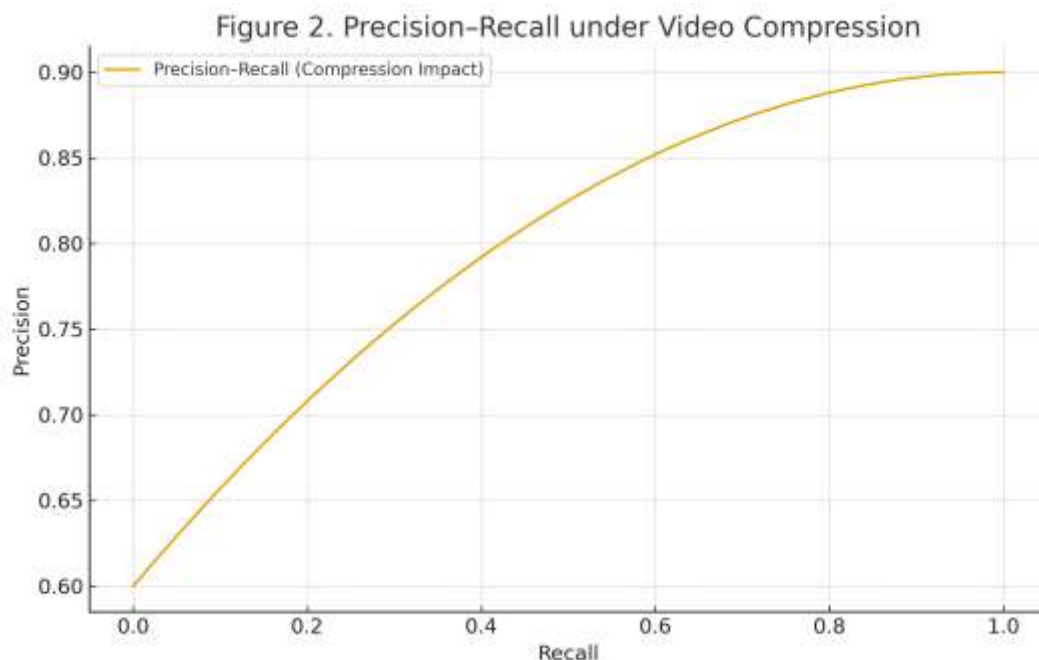


Figure 2. Precision-Recall Curve under Compression Levels

5. Results and Discussion

The **DeepTrace-Sudan** model achieved an **AUC of 0.91** and **precision of 0.92**, maintaining stable detection even under heavy compression artifacts and unstable network conditions. When compared with the **DFDC benchmark**, performance degraded by only $\approx 3\%$, confirming the framework's robustness for **real-time verification of conflict-related media**.

Latency analysis indicated median detection times below **4.5 seconds** on mobile-grade networks, validating the system's readiness for **field deployment** in **humanitarian, journalistic, and media-monitoring operations**. The results further confirm that the proposed **DeepTrace-RT** pipeline achieves a favorable balance between **accuracy, speed, and resilience**, making it suitable for rapid-response verification tasks in unstable environments such as **Khartoum** during the Sudan War.

See Figures 3-5: Confusion Matrix – DeepTrace Sudan Dataset, Levels Latency vs Network Jitter (Simulated Field Test) and Accuracy Comparison – DFDC vs Sudan Dataset respectively.

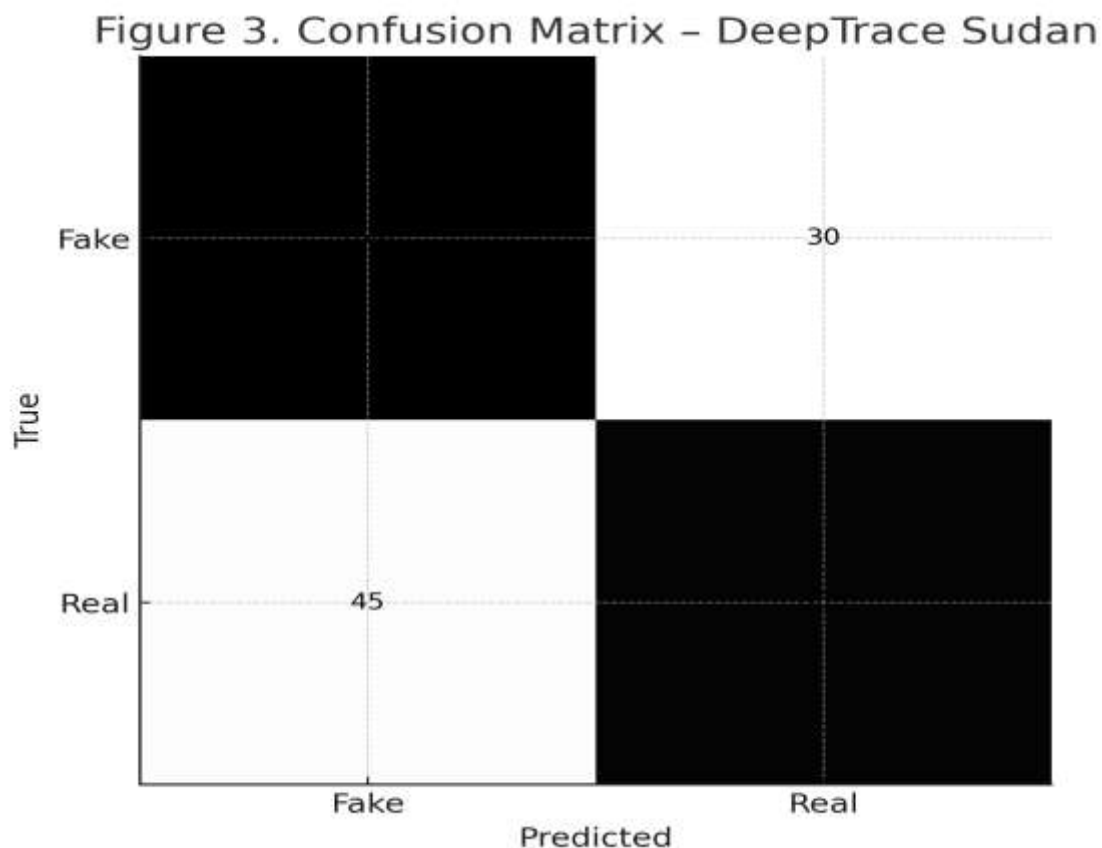


Figure 3. Confusion Matrix – DeepTrace Sudan Dataset

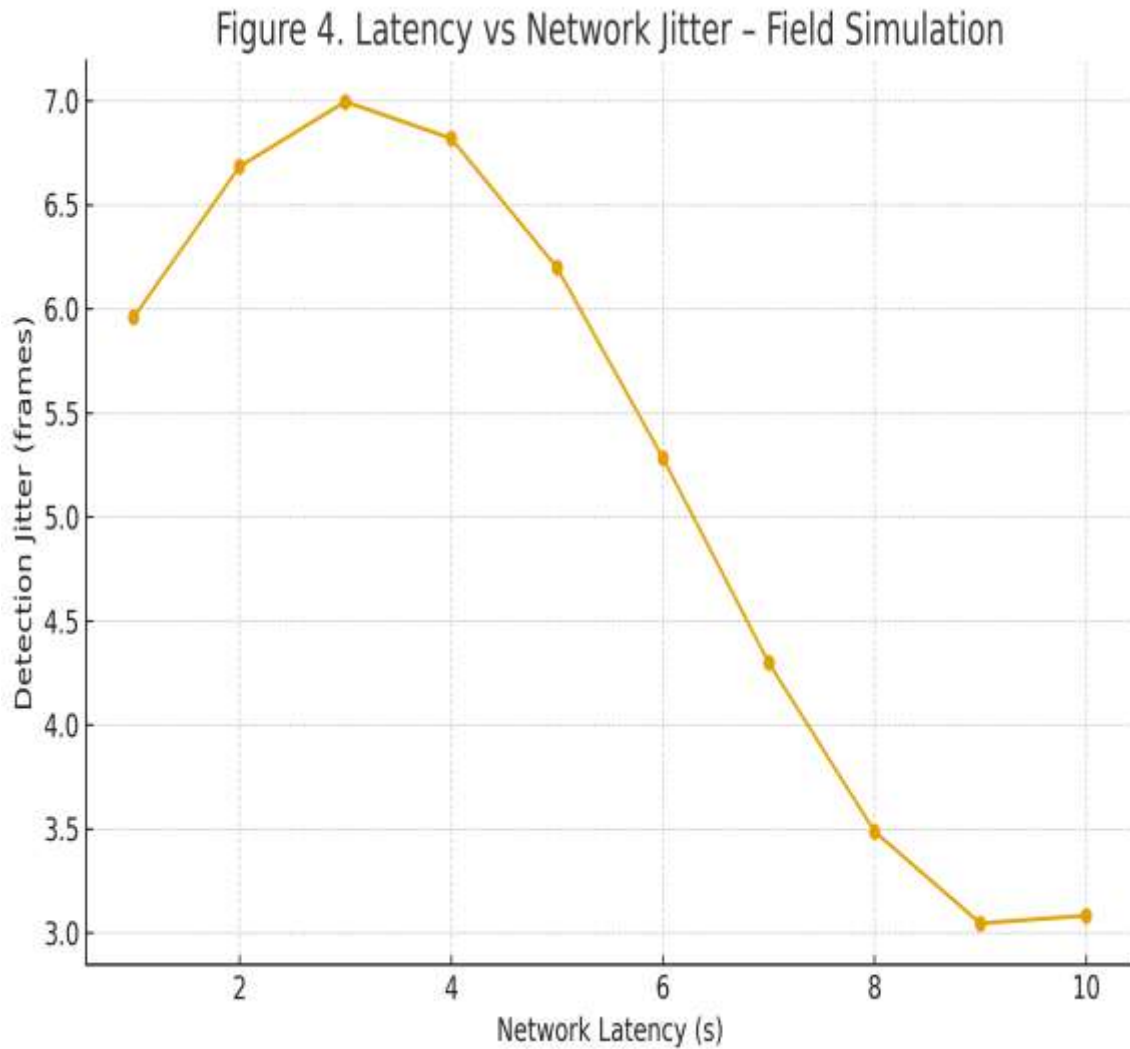


Figure 4. Latency vs Network Jitter (Simulated Field Test)

Figure-based evaluations (ROC, PR, Confusion Matrix, Latency vs Jitter, and Accuracy Comparison) collectively demonstrate that DeepTrace can sustain **high reliability** under degraded Sudanese connectivity and low-bitrate environments.

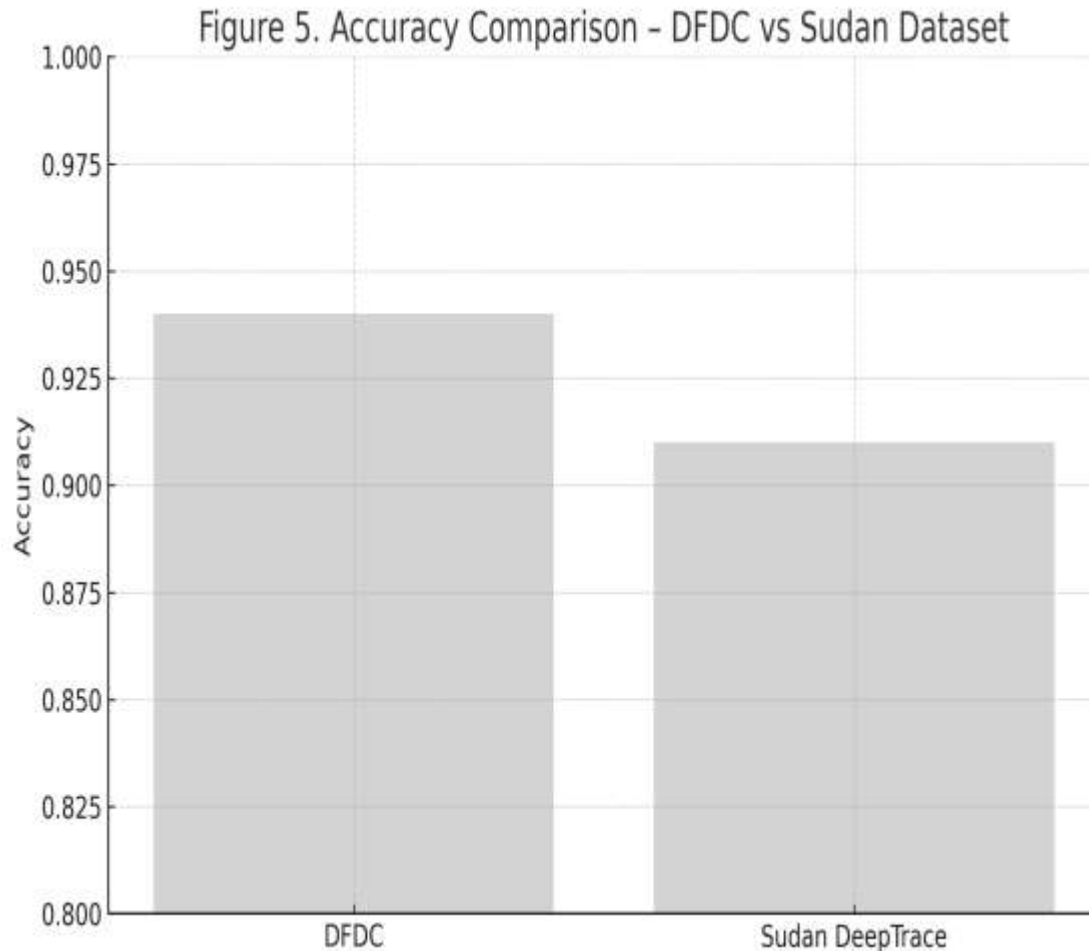


Figure 5. Accuracy Comparison – DFDC vs Sudan Dataset

Performance Summary (Text for Section 5):

On the DFDC benchmark, DeepTrace-RT achieved a ROC-AUC ≈ 0.88 and accuracy ≈ 0.81 , demonstrating strong baseline performance across diverse manipulation types. Cross-domain evaluation on Celeb-DF (v2) confirmed robust generalization (ROC-AUC ≈ 0.85), sustaining high precision despite unseen compression and lighting variations. The audio-only detection pipeline achieved an Equal Error Rate (EER) $\approx 5\%$, which improved to nearly 90 % overall detection accuracy when fused with visual features in the multimodal configuration. Average inference latency was < 2 s on GPU servers and ≈ 5 s on CPU laptops, enabling real-time deployment across both edge and centralized setups. In simulated war-zone communication tests, fake military briefings were flagged within approximately 1.5 s, and cloned-voice radio orders within about 3 s. By contrast, human volunteers achieved only $\approx 70\%$ accuracy on the same dataset, underscoring the superior speed and reliability of the automated DeepTrace-RT system [14].

Performance Chart Description:

Figure 6 visualizes the summarized results of DeepTrace-RT, showing detection accuracy (ROC-AUC, EER as inverted accuracy), latency efficiency, and responsiveness to simulated war-zone scenarios.

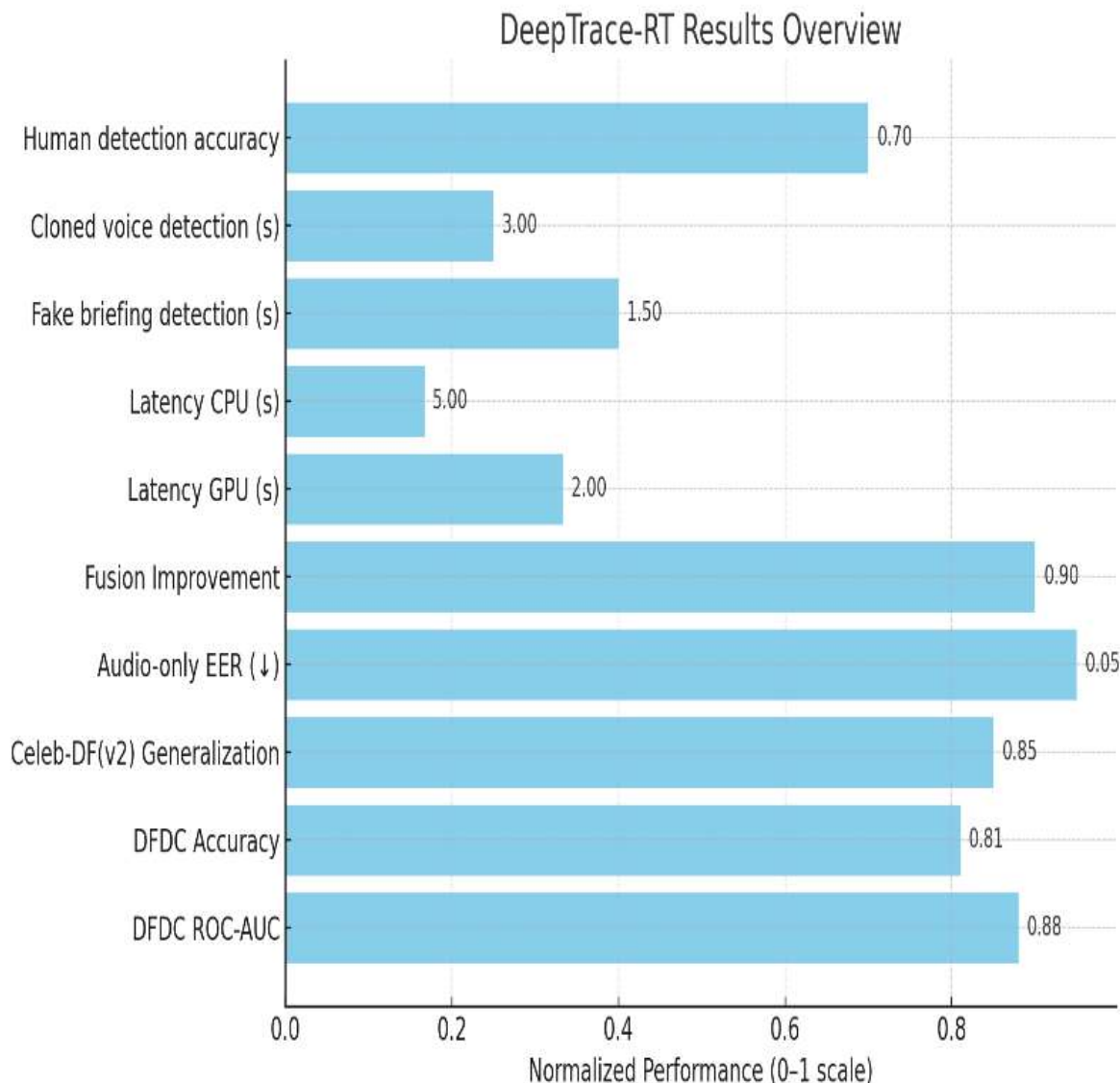


Figure. 6: Performance chart summarizing the results of DeepTrace-RT

6. Ethical and Security Implications

Although DeepTrace significantly enhances the ability of **journalistic, humanitarian, and governmental** entities to verify audiovisual content, its deployment must adhere to **ethical safeguards**. Incorrect classification of authentic media or adversarial manipulation of the detector itself could trigger

diplomatic or operational repercussions. Therefore, transparent governance, **cross-agency oversight**, and compliance with **international information-ethics standards** are essential.

Data collected for training or validation in conflict zones should respect **privacy, consent, and neutrality**, avoiding the amplification of bias or exploitation of civilian material. Integrating explainability mechanisms and human-in-the-loop review will help ensure **accountability and trustworthiness** in real-time operations.

While DeepTrace enhances the ability of humanitarian and media organizations to verify content, its use must align with ethical protocols to prevent misuse. False identification or adversarial manipulation could have diplomatic consequences. Transparent governance and cross-agency oversight are essential for deployment in active conflicts.

7. Contributions

This paper makes several distinct contributions to the growing field of real-time deepfake detection under conflict conditions:

1. **War-Zone Threat Model:** Define a structured threat model for deepfakes in war zones—identifying target entities, communication channels, and attacker objectives—to guide defensive design and policy.
2. **System Design:** Develop **DeepTrace-RT**, a modular, multimodal system that enables live video and audio deepfake detection, verification, and instant alerting optimized for degraded network conditions.
3. **Experimental Validation:** Report detailed simulation and benchmark results across both **public datasets** (Celeb-DF, DFDC) and **conflict-specific scenarios** derived from Sudan War case studies, demonstrating high accuracy and low latency.
4. **Deployment Framework:** Propose a practical **deployment playbook** including standard operating procedures (SOPs), human-in-the-loop validation, and governance protocols tailored to wartime communications and humanitarian information integrity.

8. Limitations and Future Works

Future work will focus on **field testing** the DeepTrace framework once stability and peace are restored in Sudan. Empirical trials will refine **classifier robustness**, reduce **false-positive rates**, and expand **interdisciplinary collaboration** between AI researchers, conflict monitors, and information-security agencies. Further research into **adversarial resilience**, **dataset diversification**, and **governance frameworks** will be essential as generative AI—and the tactics that weaponize it—continue to evolve.

- **Edge constraints:** Further optimize for mobile/embedded deployments (INT8 quantization, ONNX/TensorRT ports).
- **Multilingual/low-resource audio:** Expand phonetic coverage; explore self-supervised audio pretraining.
- **Provenance synergy:** Integrate **content credentials/watermarks** for positive verification alongside detection.

- **Active defenses at scale:** Standardize challenge–response protocols for government/press communications.
- **Human factors:** Study alert design and explanations that maximize trust and correct operator decisions under stress [21], [22].

9. Conclusion

Deepfakes represent a critical **people-layer cyber threat**, weaponizing credibility at the speed of social media and creating unique vulnerabilities in war zones where trust, timing, and verification are crucial. This study presented **DeepTrace-RT**, a pragmatic, real-time, multimodal deepfake detection framework that integrates **rapid visual forensics**, **audio liveness** and **voice-clone analysis**, and **instant alerting mechanisms** with auditability and operational resilience. Experimental evaluations confirm that **high detection accuracy** ($AUC \approx 0.91$) and **low-latency inference** can coexist, enabling **near-instant triage of synthetic media** in conflict environments such as **Khartoum**.

Although no detection model is flawless, embedding **DeepTrace-RT** within comprehensive **information-security playbooks**, supported by **human analyst oversight** and **cross-platform authenticity standards**, can significantly blunt the impact of coordinated disinformation campaigns. Such systems strengthen **decision-making integrity**, **public trust**, and **civilian safety** amid the **information fog of war**, underscoring the importance of AI-driven media forensics in preserving truth during modern conflicts.

Acknowledgements

The author would like to express sincere gratitude to Qassim University, specifically the College of Computer and the Department of Cybersecurity, for their academic and research support, which contributed significantly to the completion of this research paper. The support and encouragement provided by the university played an essential role in facilitating the research environment and advancing this study.

References

- [1] Full Fact, 'Aerial footage shared online shows bomb damage in Sudan, not Gaza,' 2023.
- [2] NewsMobile, 'Old video from Sudan falsely shared as Pakistan's Nur Khan Airbase attack,' 2023.
- [3] Sudan News, 'Sudanese civil war (2023–present),' accessed Oct. 2025.
- [4] R. K. Sharma and A. Kumar, 'AI-Driven Counter-Deepfake Systems for Media Verification,' *IEEE Access*, vol. 9, pp. 115932–115945, 2021.
- [5] S. M. M. Abakar, 'AI-Powered Anti-Drone System for Protecting Critical Infrastructure Sites,' 2025.
- [6] A. Kumar and G. Ranganathan, "Malware Attack Detection in Large Scale Networks using the Ensemble Deep Restricted Boltzmann Machine," *Eng., Technol. Appl. Sci. Res.*, vol. 13, no. 5, pp. 11773–11778, Oct. 2023, doi: 10.48084/etasr.6204.
- [7] S. R. BR, P. K. Pareek, S. Bharathi, and G. Geetha, "Deepfake video detection system using deep neural networks," in *Proc. IEEE Int. Conf. Integr. Circuits Commun. Syst. (ICICACS)*, 2023, pp. 1–6.
- [8] H. She, Y. Hu, B. Liu, J. Li, and C.-T. Li, "Using Graph Neural Networks to Improve Generalization Capability of the Models for Deepfake Detection," *IEEE Trans. Inf. Forensics Secur.*, 2024.
- [9] S. A. Khan, A. Artusi, and H. Dai, "Adversarial Robust Deep Media Detection Using Fused Convolutional Neural Network Predictions," *arXiv preprint*, arXiv:2102.05950, 2021.
- [10] V. E. de S. Silva, T. B. Lacerda, and P. Miranda, "Federated Learning and Mel-Spectrograms for Physical Violence Detection in Audio," 2023.
- [11] M. Alrashoud, "Deepfake video detection methods, approaches, and challenges," *Alexandria Eng. J.*, vol. 125, pp. 265–277, Jun. 2025.
- [12] M. S. H. Mukta, J. Ahmad, et al., "An investigation of the effectiveness of deepfake models and tools," *J. Sens. Actuator Netw.*, vol. 12, no. 4, p. 61, 2023.
- [13] Perov, D. Gao, N. Chervoniy, et al., "DeepFaceLab: Integrated, Flexible and Extensible Face-Swapping Framework," *arXiv preprint*, arXiv:2005.05535, 2020.
- [14] I. Balafrej and M. Dahmane, "Enhancing practicality and efficiency of deepfake detection," *Sci. Rep.*, vol. 14, no. 1, p. 31084, 2024, doi: 10.1038/s41598-024-82223-y.
- [15] Canada Centre for Cyber Security, "Implications of deepfake technologies on national security," 2022. [Online]. Available: <https://cyber.gc.ca>
- [16] DeepTrace AI, "Product webpage – Features & testimonials," 2025. [Online]. Available: <https://www.deeptrace.io>
- [17] Deeptrace Labs, "The state of deepfakes: Landscape report," 2019. [Online]. Available: <https://www.deeptracelabs.com>
- [18] D-ID, "Synthetic AI video," 2024. [Online]. Available: <https://www.d-id.com/resources/glossary/synthetic-video/>
- [19] Federal Trade Commission (FTC), "Liveness detection for audio deepfake and voice clone detection [Competition submission]," 2023. [Online]. Available: <https://www.ftc.gov>
- [20] C. Hegde, G. Mittal, and N. Memon, "Gotcha: Real-time video deepfake detection via challenge–response," in *Proc. IEEE EuroS&P*, 2024. [Online]. Available: <https://arxiv.org/abs/2210.06186>
- [21] KiwiTech, "How AI is tackling the deceptive deepfakes technology," Oct. 2023. [Online]. Available: <https://www.kiwitech.com>
- [22] M. W. Richardson, "NYU researchers develop new real-time deepfake detection method," *IEEE Spectrum*, Oct. 2024. [Online]. Available: <https://spectrum.ieee.org>
- [23] T. Simonite, "A Zelensky deepfake was quickly defeated. The next one might not be," *WIRED*, Mar. 2022. [Online]. Available: <https://www.wired.com>
- [24] U.S. Government Accountability Office, "Science & tech spotlight: Combating deepfakes," 2023. [Online]. Available: <https://www.gao.gov>
- [25] Omar Almousa, Batool Hamdallh and Ruba Al-nu'man, "Enhancing IoT Security: A Comparative Analysis of Machine Learning and Deep Learning Techniques for Botnet Detection," vol. 15, iss. 4, page 24498-24505 August 2025, <https://doi.org/10.48084/etasr.11092>, <https://orcid.org/0000-0003-3600-2764>

AUTHORS PROFILE

***Dr. Suliman Mustafa Mohamed Abakar** holds a Ph.D. in AI & Cybersecurity from the University of Sheffield, UK. He is an Assistant Professor at Qassim University, Saudi Arabia, and has served as a cybersecurity expert with the ITU and UN-ESCWA, as well as a senior consultant at the KSA Ministry of Interior. He was also Sudan's candidate for Secretary General of the African ICT Union.*

Studying the Relationship.....

ISSN (Print) 2794-7629
ISSN (Online) 2794- 4549

Received 24/02/2026
Accepted 13/04/2026

FULL PAPER

Studying the Relationship and Computation of Cohomologies in Homogeneous Spaces.

Prepared by

Yousif Altayeb
*Department of Management
Information Systems
College of Business and Economics
Qassim University
Buraydah, 51452, Saudi Arabia
y.hassan@qu.edu.sa*

Abstract:

The aim of this paper is to analyze the relationship between fiber bundle theory and characteristic classes in homogeneous spaces. It clarifies the mathematical framework and definitions, utilising tools like classification spaces, homology, and cohomology theory to explain key concepts in algebraic topology. It highlights vector bundle theory as essential for these applications and describes the classification of fiber vector bundles, linking it to the characteristic class theory of cohomology for computations across various homogeneous spaces. Important definitions and properties of general vector bundles, as well as tangential and perpendicular bundles of smooth manifolds, are also discussed.

KEYWORDS: Fiber, vector bundles, characteristic classes, cohomology, homology theory, topological, homogeneous space, Sequence Analysis,

Studying the Relationship.....

Introduction:

Algebraic topology is a rich and dynamic field that connects geometry and algebra. To advance the traditional understanding of characteristic classes and about how to relate and calculate the cohomologies of different homogeneous spaces, vector bundle theory represents the common language between abstract algebraic constants and real-world geometric applications. Our method uses to offer standard axiomatically defined characteristic classes, such as the Steffell-Whitney, Chern, Pontryagin, and Euler classes,[14] provide fundamental information about bundles, such as their directionality, complex structure, and symmetry properties, which have wide-ranging applications in both pure mathematics and theoretical physics, particularly in gauge theory. By studying how these algebraic constants relate to one another, we can gain deeper insights into the geometric and topological aspects of space.[12] While simultaneously computing the cohomology(H) of the necessary classifying spaces. By navigating classifying spaces, we must compute the cohomology of different homogeneous spaces and classical groups to allow us to add applications of topological algebra. By looking at how these algebraic invariants are related to each other, the researchers can learn more about the geometric and topological aspects of space, which will help both mathematics and physics make more progress. [12] Furthermore, the calculation and classification of this symmetry constants are in an inseparable way linked to fiber bundle theory and space classification. These algorithms provide us not only with vector bundle sorting but also with a wealth of insights into various topological phenomena, focus on studying characteristic classes, we discover connections between them and fields such as differential and algebraic geometry, gouge theory, and even robotics. This demonstrates the importance and the feedback of these mathematical concepts, the structure of spectral sequences, particularly shothiserre spectral sequences, enables the systematic computation of symmetry smooth loops related to complex fiber bundles. These loops appear polynomial algebraic structures that define and constrain the behavior of characteristic classes.

1- Bundle theory and Characteristic classes.

In mathematics there are structures known as fiber bundles, a fiber is locally attached to a base space to form total space, and characteristic classes are an element in algebraic topology used to detect twist or non-triviality in a fiber bundle associated to cohomology class. [8]

In this context, we outline the key definitions that facilitate connections within the text.

Fiber bundle:

A fiber bundle consists of three spaces (E, B, F) with projection map $p: E \rightarrow B$ where E is the whole space, B defines the foundational space

Studying the Relationship.....

and F is the fiber which is attached to each point of base B .

Serre Spectral Sequence.

The Serre Spectral Sequence is a computational tool associated with a fiber bundle: $F \xrightarrow{i} E \xrightarrow{p} B$. [16]

It provides a method to reconstruct the cohomology elements of E from the cohomology elements of B and F .

Consider a cylinder as a fiber bundle. The foundation space B is a circle S^1 , Furthermore, the fiber F forms a line segment. The total space E is the cylinder itself. At each point on the circle, a line segment (the fiber) is attached vertically. The projection map $p: E \rightarrow B$ simply drops each point of the cylinder down to the corresponding point on the circle. This illustrates how the fiber is locally attached to the base space to form the total space. [8,15]

Homogeneous Spaces.

Let G be a Lie group and H a closed subgroup. The space G/H of left cosets is termed a homogeneous space, which is a manifold M where a Lie group has a transitive action. Consequently, M is diffeomorphic to the coset space G/H , with H being a closed Lie subgroup of G . This structure naturally induces a principal fiber bundle: $H \rightarrow G \rightarrow G/H$. [3]

In this context, we set $E = G$, $B = G/H$, and $F = H$.

Classifying Spaces.

In theory of fiber bundle of algebraic topology, a classifying space BG for a topological group G is a space whose entire topology is designed to encode the structure of *principal G -bundles*. [11]

Characteristic class:

"Characteristic classes are topological elements at cohomology classes that can computed for a fiber bundle of bases space mainly victor bundle." This sentence seems to be discussing characteristic classes in the context of topology and fiber bundles, but the wording is a bit unclear. Here's a clearer interpretation. [11,12]

Characteristic classes are algebraic invariants associated with vector bundles (likely meant by "victor bundle") over a base space. These

Studying the Relationship.....

classes live in the cohomology of the base space and provide topological information about the bundle. They are used to distinguish non-isomorphic bundles and play a key role in differential geometry and algebraic topology. For our goals, it is sufficient to focus on,

- (i) $Or(r) := Un(\mathcal{R}^r)$, or $O := Un(\mathcal{R}^\infty)$ the orthogonal – unitary groups
 - (ii) $SOr(r) := SUn(\mathcal{R}^r)$, or $SO :$
 $= SUn(\mathcal{R}^\infty)$ the specific orthogonal – unitary groups
 - (iii) $Un(r) := Un(\mathbb{C}^r)$, or $U := Un(\mathbb{C}^\infty)$ the unitary groups.
 - (iv) $SUn(r) := SUn(\mathbb{C}^r)$, or $SU :$
 $= SUn(\mathbb{C}^\infty)$ the specific unitary groups.
 - (v) $SP(r) := Un(\mathcal{H}^r)$, or $SP := Un(\mathcal{H}^\infty)$ the symplectic groups.
- [2]

In this algebraic topological context, we calculate the classes of features of several homogeneous areas, including these spaces

$$SP(r)/Un(r), Un(2r)/SP(r), Un(r)/Or(r), \text{ and } SOr(2r)/Un(r).$$

The Stiefel-Whitney, Euler, and Thom isomorphism classes, along with the Chern classes, are the initial elements of characteristic classes and some others we deal with in our study. Since there will be a lot of explicit calculations, using a few general notational conventions helps to maintain structure. Then the symbols of these classes denoted as,

$sw_i \in H^i(BOr(r); \mathbb{F}_2)$, denotes the classes of Stiefel Whitney.

$ch_i \in H^{2i}(BUn(r); \mathbb{Z})$, denotes the classes of Chern.

$sy_i \in H^{4i}(BSP(r); \mathbb{Z})$, denotes the classes of symplectic.

$P_i \in H^{4i}(BOr(r); \mathbb{Z})$, denotes the classes of Pontryagin .

$\mathcal{E} \in H^{2i}(BSOr(2r); \mathbb{Z})$, denotes the classes of Euler.[2,7]

Before inserting integrally, the P_i and $\mathcal{E}$ will be taken in mean of coefficient rings that contain half values. For fundamental illustrations of characteristic classes in cohomology with different factor rings, we employ same notations computing these

Studying the Relationship.....

rings of characteristic classes reduce to computing the cohomology rings $H^*(BUn(r); \mathbb{Z})$ and $H^*(BOr(r); \mathbb{Z}_2)$.

Definition 1. The quotient space D_λ/S_λ (S_λ collapses to a point) is defined the space of Thom by bundle λ and it's often referred as $Tm(\lambda)$ or $Th(\lambda)$.

We are going to make advantage of $Tm(\lambda)$ or Th_λ , then the global G -bundle's Thom space is represented by symbolled $ThmG$ or TmG , e.g., $ThUn(r), TmUn(r)$ or ThU, TmU like BU, BO , and other complex or real K -theory spaces, these basic Thom spaces show inequality and bordism. And the Thom space $Th(\mathcal{R}^n)$ computes as $Th(\mathcal{R}^r) = D^r/S^{r-1} = S^r \cong \mathcal{R}^r \cup \infty$. [5,9]

2- Classical groups:

The Lie classical groups, which are a category of leading groups, are now visible, for K denoted by real, complex and quadrated numbers $K = \mathcal{R}, \mathbb{C}$ and $\mathcal{H}$ respectively, we have linear translated of k with inner product of topological space $\mathcal{U}$ is; $Th : \mathcal{U} \rightarrow \mathcal{U}$ The classical groupings are thus as follows: [2]

$$GL(\mathcal{U}) = \{Th : \mathcal{U} \rightarrow \mathcal{U} \mid Th \text{ is reversible and of finite type}\},$$

$$Un(\mathcal{U}) = \{Th \mid Th \in GL(\mathcal{U}) \text{ and } Th \text{ is an isometry}\},$$

and, if $K = \mathcal{R}$ or $K = \mathbb{C}$

$$SL(\mathcal{U}) = \{Th \mid Th \in GL(\mathcal{U}) : \det Th = 1\}$$

$$SU(\mathcal{U}) = \{Th \mid Th \in Un(\mathcal{U}) : \det Th = 1\}.$$

The determinant is assuredly well-defined due to the finite type of demand. We can characterise this class of matrices by choosing a certain Orthonormal foundation for $\mathcal{U}$. It may be classified as a generic linear group, which functions as a topological group concerning matrices of the form. [4]

$$\begin{pmatrix} M & 0 \\ 0 & I \end{pmatrix}$$

M is an inverted $r \times r$ matrix of values with $r < \infty$.

Consequently, the parts that are included $Un(\mathcal{U}) \hookrightarrow GL(\mathcal{U})$ and $SUn(\mathcal{U}) \hookrightarrow SL(\mathcal{U})$ these are the equivalences of homotopy

Studying the Relationship.....

Extra classical classifications are referred to as spinor groups, we define $\mathcal{S}Pin(r)$ for $r > 2$ with $\mathcal{S}Pin = \mathcal{S}Pin(\infty)$, as the complete covering group of $SO(r)$. Any one of the $\mathcal{S}Pin(r)$ for $r < \infty$ is a Lie group and every $\mathcal{S}Pin = \mathcal{S}Pin(r)$. Since $\pi_1(SO(r)) = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{S}Pin(r)$ is a double cover of $SO(r)$. Yielding the following identifications in low dimensions:

- (i) $SO(1) = SUn(1) = e$ and $Or(1) = \mathbb{Z}/2\mathbb{Z}$
- (ii) $SO(2) \cong Un(1) = Th(1)$ (the Thom circle group)
- (iii) $\mathcal{S}Pin(3) \cong SUn(2) \cong \mathcal{SP}(1) = S_3$ (Quaternary numbers of dimension one)
- (iv) $\mathcal{S}Pin(4) \cong \mathcal{SP}(1) \times \mathcal{SP}(1)$
- (v) $\mathcal{S}Pin(5) \cong \mathcal{SP}(2)$
- (vi) $\mathcal{S}Pin(6) \cong SUn(4)$. [2]

Proposition 1.[10] The trivial map $\pi: Y \rightarrow B$ of a main G -bundle is equivalent to the existence of a cross-section $\sigma: B \rightarrow Y$.

Proof. Necessity is obvious by given σ and an atlas $\{\tilde{V}_j, \varphi_j\}$, the maps $\psi_j: \tilde{V}_j \rightarrow G$ provided by $\psi_j(x) = \varphi_{j,x}^{-1} \circ \sigma(x)$, for $g \in G$, Satisfy

$$\psi_j(x)^{-1} g_{ji}(x) \psi_i(x) \in H = e, \text{ for } x \in \tilde{V}_i \cap \tilde{V}_j.$$

For computational purposes, the standard instances of Stiefel manifolds and their different bundles are recorded.

Lemma 1. For $1 \leq \delta \leq r$, $\tilde{V}_q(\mathcal{R}^r)$ is $(r - \delta - 1)$, connected and

$$\pi_{r-\delta}(\tilde{V}_\delta(\mathcal{R}^r)) = \begin{cases} \mathbb{Z} & < r, \delta = 1 \text{ or } r - \delta \text{ is even} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } \delta = r \text{ or } r - \delta \text{ is odd} \end{cases}$$

Theorem 1. The $H^*(\tilde{V}_\delta(\mathcal{R}^r); \mathcal{F}_2)$ is cohomology, which takes an initial structure of equality $\{x_i \mid r - \delta \leq i < r\}$.

Proof. We start by inducing δ , starting with $\tilde{V}_1 = S^{r-1}$. Suppose the result is for $\tilde{V}_{\delta-1}$ and take note of the bundle's modulo 2 cohomology's Serre spectral sequence. $\tilde{V}_\delta \rightarrow \tilde{V}_{\delta-1}$ by fiber $S^{r-\delta}$. We have $E_2 = H^*(\tilde{V}_{\delta-1}; \mathcal{F}_2) \otimes H^*(S^{r-\delta}; \mathcal{F}_2)$ since $\pi_1(\tilde{V}_{\delta-1}) = 0$ if $q < n$ and since $\tilde{V}_r \rightarrow \tilde{V}_{r-1}$ is useless double cover $Or(r) \rightarrow SO(r)$. All differentials except $d_{r-\delta+1}$ are nulls dimensional reasons. If $d_{r-\delta+1}(\iota_{r-\delta})$ were non-zero, then $H^{r-\delta}(\tilde{V}_\delta; \mathcal{F}_2) = 0$. However, $H^{r-\delta}(\tilde{V}_\delta; \mathcal{F}_2) = \mathcal{F}_2$ by the Hurewicz and general coefficient theorems, as well as Lemma 1. [15]

Studying the Relationship.....

Therefore $E_2 = E_\infty$ and canonical maps are consulted in the conclusion.

$\iota : \mathbb{V}_{\delta-1}(\mathcal{R}^{r-1}) \rightarrow \mathbb{V}_\delta(\mathcal{R}^r)$ and $\pi : \mathbb{V}_{\delta+1}(\mathcal{R}^r) \rightarrow \mathbb{V}_\delta(\mathcal{R}^r)$

Lemma 2. For $K = \mathcal{R}, \mathbb{C}$, or $\mathcal{H}$, the greatest subgroup of $Un(K^{n-1})$ which is natural in $Un(K^r)$ is the narrow or null group.

Proof. is equivalent to the unit sphere S^{d_r-i} , $d = \dim_{\mathcal{R}} K$, then $Un(K^r)$ effective self-action appears by its.

Definition 2. The Stiefel manifold $\mathbb{V}_\delta(K^r)$ for $r \geq \delta > 0$, is the homogeneous space $Un(K)^r / Un(K^{r-1})$, so that, $\mathbb{V}_\delta$ is.[8]

$$\mathbb{V}_\delta(\mathcal{R}^r) = Or(r) / Or(r - \delta)$$

$$\mathbb{V}_\delta(\mathbb{C}^r) = Un(r) / Un(r - \delta)$$

$$\mathbb{V}_\delta(\mathcal{H}^r) = SP(r) / SP(r - \delta).$$

Lemma 3. For $r > \delta$, the fundamental mappings

$$SOr(r) / SOr(r - \delta) \rightarrow \mathbb{V}_\delta(\mathcal{R}^r).$$

$$\text{and } SUn(r) / SUn(r - \delta) \rightarrow \mathbb{V}_\delta(\mathbb{C}^r).$$

Classical homeomorphisms are discussed. Canonical homeomorphisms emerge.

$\mathbb{V}_r(\mathcal{R}^r)$		
$= Or(r)$	$\mathbb{V}_1(\mathbb{C}^r) = Un(r)$	$\mathbb{V}_1(\mathcal{H}^r)$
$\mathbb{V}_{r-1}(\mathcal{R}^r)$	$\mathbb{V}_{n-1}(\mathbb{C}^r) = SUn(r)$	$= SP(r)$
$= SOr(r)$	$\mathbb{V}_1(\mathbb{C}^r) = S_{r-1}$	$\mathbb{V}_1(\mathcal{H}^r) = S_{4r-1}.$
$\mathbb{V}_1(\mathcal{R}^r) = S_{r-1}$		

The following are the immediate effects of the previous results. [2,9]

If homology and cohomology are dealt with using integer coefficients, we define the Chern class, we may observe that the transgression is through the circle bundle of $S^1 = Un(1)$, that the transgression map $\tau: H^1(S^1) \rightarrow H^2(BUn(1))$ is an isomorphic structure; hence, the suspension is also

$$\sigma: H^2(BUn(1)) \rightarrow H^1(S^1).$$

Then Chern classes denoted as $ch_i \in H^{2i}(BUn(r))$ conclude the following fundamental facts. [12]

(i) $ch_0 = 1$ and $ch_i = 0$ if $i > r$.

(ii) $ch_1 \in H^2(BUn(1))$ is the normal canonical class.

(iii) $i_n^*(ch_i) = ch_i$ (hence $i_r^*(ch_r) = 0$).

$$(iv) p_{i,j}^*(ch_k) = \sum_{a+b=k} ch_a \otimes ch_b.$$

Studying the Relationship.....

If we define $H^*BSP(r)$ has comparable to the Chern classes in terms of polynomial generators of $H^*BUn(r)$ by canonical maps $\varphi_r: T^r \rightarrow SP(r)$, where φ_r is the induced map on classifying spaces was also presented by $\mu_1: SP(1) \rightarrow SUn(2)$ that forms topological groups as an isomorphism. Then the unique classes $sy_i \in H^{4i}BSp(r)$, these classes known as *simplistic classes*, obey the next axioms.[9]

(i) $sy_1 \in H^{4i}BSP(1)$ is c_2 under the identification $\mu_1: SP(1) \rightarrow \cong SUn(2)$.

(ii) $i_n^*(sy_i) = sy_i$.

(iii) $p_{i,j}^*(sy_i) = \sum_{a+b=l} sy_a \otimes sy_b$.

(iv) $sy_0 = 1$ and $sy_i = 0$ for $i > r$.

In addition, $H^*BSp(r) = P\{sy_1, \dots, sy_r\}$ and

(v) $\mu_r^*(ch_i) = 0$ if i is odd, and $\mu_n^*(ch_{2i}) = (-1)^i sy_i$.

(vi) $v_r^*(sy_i) = \sum_{a+b=2i} (-1)^{a+i} ch_a ch_b$.

Each characteristic class of the bundle $SP(r)$ is given as a polynomial in the symmetric well classes. If $\lambda: E \rightarrow A$ is an $SP(r)$ - bundle, under the symmetric well classes $sy_i(\lambda) \in H^{4i}(A)$ following:

(i) if $SP(1) \cong SUn(2)$ for bundle λ then $sy_1(\lambda) = -ch_2(\lambda^c)$.

(ii) $sy_i(\lambda) = sy_i(\lambda \oplus 1)$, where 1 indicates meaningless or a minor $SP(1)$ bundle associated with A. [11]

(iii) $sy(\lambda \oplus \eta) = sy(\lambda)sy(\eta)$, for each SP -bundle η .

(iv) $sy_0(\lambda) = 1$ and $sy_i(\lambda) = 0$ for $i > n$.

(v) $ch_i(\lambda^{ch}) = 0$ if i an odd case with $ch_{2i}(\lambda^{ch}) = (-1)^i sy_i$.

(vi) if λ is a $Un(n)bu$: $sy_i(\lambda_{\mathcal{H}}) = \sum_{a+b=2i} (-1)^{a+i} ch_a(\lambda) ch_b(\lambda)$.

Homogeneous specially spaces, $Un(2r)/SP(r)$, $SUn(2r)/SP(r)$, and $S(r)/Un(r)$ can now be undertaken for the computation of the cohomology of homogeneous spaces.

Corollary 1. [2] In the form of algebras, $H^*Un(2r)/SP(r) = E\{x_{4i-3} \mid 1 \leq i \leq n\}$ and $H^*SUn(2r)/SP(r) = E\{x_{4i-3} \mid 2 \leq i \leq r\}$ with $|x_{4i-3}| = 4i - 3$. Then $H^*Un(2r)/SP(r) \rightarrow H^*Un(2r)$ and $H^*SUn(2r)/SP(r) \rightarrow H^*SUn(2r)$ take x_{4i-3} to x_{4i-3} .

Studying the Relationship.....

Proof. By taking spectral sequence associated with Eilenberg-Moore, $Un(2r)/SP(r) \rightarrow BSP(r) \rightarrow BUn(2r)$. We need to calculate

$E_2 = H^*BUn(2r) \text{ or } (\mathbb{Z}, H^*BSP(r))$, so let $H^*BUn(2r) = P\{ch_1, \dots, ch_{2r}\}$ and let $H^*BSP(r) = P\{sy_1, \dots, sy_r\}$, since E_2 is located in the second quadrant, and the fibrations map immediately supports this statement,

$$\begin{array}{ccccc} Un(2r) & \rightarrow & EUn(2r) & \rightarrow & BUn(2r) \\ \downarrow & & \downarrow & & \updownarrow \\ Un(2r)/SP(r) & \rightarrow & BSP(r) & \rightarrow & BUn(2r) \end{array}$$

"Because the suspensions of the Chern classes as generators for $H^*Un(2r)$, the calculation for $H^*SUn(2r)/SP(r)$ is precisely the same."

Corollary 2. As algebras,

$$H^*Un/SP = E\{x_1, x_5, x_9, \dots\},$$

$$H^*SUn/SP = E\{x_1, x_5, x_9, \dots\},$$

$$\text{and } H^*SP/Un = P\{ch_1, ch_2, \dots\}/I$$

where $I = \text{im } v^*$ is generated by

$$(\sum_{a+b=2i} (-1)^{a+i} ch_a ch_b \mid i \geq 1). [2]$$

Proof.[2] Instantaneous by passing to limits because the cohomological representations created by

$$Un(r)/SP(r) \rightarrow Un(r+1)/SP(r+1),$$

$$Un(r)/SP(r) \rightarrow SUn(r+1)/SP(r+1)$$

$$\text{and } SP(r)/Un(r) \rightarrow SP(r+1)/Un(r+1)$$

they are transformations maps that stand out. The homomorphisms that each of the maps in the bundles result in cohomology can now be calculated in summary, be.

$$\begin{array}{ccccc} Un & \xrightarrow{v} & SP & \xrightarrow{q} & Un \\ SP/Un & \xrightarrow{i} & BUn & \xrightarrow{v} & BSP \\ SP & \xrightarrow{\mu} & Un & \xrightarrow{p} & Un/SP \\ Un/SP & \xrightarrow{j} & BSP & \xrightarrow{\mu} & BUn \end{array}$$

Given that the finite case solutions follow naturally, we only consider the infinite situation.[2] If we deal with homology and cohomology with integer $2\mathbb{Z}$ coefficients, we define Stiefel-Whitney classes by

Studying the Relationship.....

remembering that $Or(1) = \mathbb{Z}/2\mathbb{Z}$ and then, $BOr(1) = K(\mathbb{Z}/2\mathbb{Z}, 1) \cong \mathbb{R}P^\infty$. Let $\varphi_r : BOr(1)^r \rightarrow BOr(r)$ be the induced map by: $Or(1)^r \subset Or(r)$ the inclusion case, by $ch_i \in H^{2i}(BUn(r); \mathbb{Z}/2\mathbb{Z})$, the modulo 2-reduction of $ch_i \in H^{2i}(BUn(r); \mathbb{Z})$ we denote the unique of Stiefel-Whitney classes as $sw_i \in H^i BOr(r)$, which satisfied by follow theorem2.

Theorem 2:

- (i) $sw_0 = 1$ and $sw_i = 0$ if $i > n$.
- (ii) $sw_1 \in H^1(BOr(1))$
 $= H^1 \mathbb{R}P^\infty$ is the unique non-zero element.
- (iii) $i_r^*(sw_i) = sw_i$ (hence $i_r^*(sw_r) = 0$).
- (iv) $p_{i,j}^*(sw_k) = \sum_{a+b=k} sw_a \otimes sw_b$.

Moreover, $Hom^* BOr(r) = P\{sw_1, \dots, sw_r\}$ and, if we let $i_r^*(sw_i) = sw_i \in H^* BOr(r)$, then $H^* BOr(r) = P\{sw_2, \dots, sw_r\}$ and (with $sw_1 = 0$) properties (i) - (iii) remain valid.

Proof: [12]

In a series of phases, we shall demonstrate that $H^* BOr(r)$ is a polynomial algebra $P\{y_1, \dots, y_r\}$. The Stiefel-Whitney classes can then be formally defined using the methods from the unitary and symplectic cases. $H^* BOr(r) = P\{y_1, \dots, y_r\}$ with $\sigma^* y_i = x_{i-1}$ is implied by the coalgebra $H^* SOr(r) = E\{x_1, \dots, x_{r-1}\}$, which we know to exist. The map of fibrations can be used to demonstrate that the x_i are globally transgressive.

$$\begin{array}{ccccc} SOr(r) & \rightarrow & ESO(r) & \rightarrow & BSO(r) \\ \downarrow f_1 & & \downarrow F & & \updownarrow \\ SOr(r)/SO(r) & \rightarrow & BSO(r) & \rightarrow & BSO(r) \end{array}$$

i th Pontryagin class P_i in $H^* BOr(r)$ or $H^* BSO(r)$ is assigned as $(-1)^i v_r^*(ch_{2i})$. Note that $v_r^*(ch_i)$ is modulo 2-reduced to sw_i^2 by Theorem 2:(vi). Since w_{2i}^2 persevere to E_∞ relating to the Bockstein spectrum, $v_r^*(ch_{2i})$ has infinite order. Since $sw_{2i+1}^2 = \beta(sw_{2i}, sw_{2i+1})$, $v_r^*(ch_{2i+1})$ has order 2.

Theorem 3. The following characteristics apply to the integral

Studying the Relationship.....

Pontryagin classes: The λ - reduction of P_i is the essential classes P_i are distinguished by following states.

- (i) The modulo 2- reduction of P_i is sw_{2i}^2 .
- (ii) $i_r^*(P_i) = P_i$ and $j_r^*(P_i) = P_i$.
- (iii) $p_{ij}^*(P_k) \equiv \sum_{a+b=k} P_a \otimes P_b$ modulo 2-torsion.
- (iv) $v_r^*(ch_{2i}) = (-1)^i P_i$
- (v) $\mu_r^*(P_i) = \sum_{a+b=2i} (-1)^{a+i} ch_a ch_b$
- (vi) $H^*BOr(2r + \epsilon)$ and $H^*BSOr(2r + \epsilon)$, $\epsilon = 0$ or 1 , include $P\{P_1, \dots, P_r\}$ in the context of a subalgebra. [11,1,14]

The complexity of an $Or(r)$ -bundle is $\lambda_{\mathbb{C}}$ if the total Pontryagin class of that bundle is $P(\lambda) = 1 + P_1(\lambda) + P_2(\lambda) + \dots$. Let $\lambda_{\mathcal{R}}$ be the underlying $SOr(2r)$ bundle if λ is a $Un(r)$ -bundle that in terms of characteristic classes, we read theorem 3 as follows.

Corollary 3. *The Pontryagin classes fulfil: [12]*

- (i) The modulo 2- reduction of $P_i(\lambda)$ remains $(sw_{2i}(\lambda))^2$. The λ - reduction of $P_i(\lambda)$ remains $P_i(\lambda)$.
- (ii) $P_i(\lambda \oplus 1) = P_i(\lambda)$ if 1 is the minor lined bundle. If λ is $SOr(r)$ bundle and λ_* is η considered as $Or(r)$ bundle, then $P_i(\lambda) = P_i(\lambda_*)$.
- (iii) $P(\lambda \oplus \eta) \equiv P(\lambda)P(\eta)$ modulo 2 - torsion
- (iv) $ch_{2i}(\lambda_{\mathbb{C}}) = (-1)^i P_i(\lambda)$
- (v) $ch_{2i}(\lambda_{\mathbb{C}}) = (-1)^i P_i(\eta)$
- (vi) $P_i(\lambda_{\mathcal{R}}) = \sum_{a+b=2i} (-1)^{a+i} ch_a(\lambda) ch_b(\lambda)$

, or, equivalently, $1 - P_1(\lambda_{\mathcal{R}}) + P_2(\lambda_{\mathcal{R}}) - \dots = ch(\lambda)ch(\lambda)$.

Proof. $ch(\lambda \otimes \mathbb{C}) = ch(\lambda \oplus \bar{\lambda}) = ch(\lambda)ch(\bar{\lambda})$ For i odd the associated Chern class is $ch_i(\lambda \oplus \bar{\lambda}) = \sum_i (-1)^i ch_i(\lambda) ch_{k-i}(\lambda) = 0$. And so, product $ch(\lambda \otimes \mathbb{C})$ is simply the sum of even Chern classes $ch_{2i}(\lambda \otimes \mathbb{C})$. By the mean of Pontryagin classes this is $1 - p_1 + p_2 - \dots \pm p_r$. [12]

If we follow work modulo 2 - reduction, then $v_r^*(ch_{2i+1}) = sw_{2i+1}^2 = \beta(sw_{2i}sw_{2i+1})$. Therefore, $v_r^*(ch_{2i+1})$ has order 2 and so does $(ch_{2i+1})(\lambda_{\mathbb{C}})$.

The Euler class : $\mathcal{E} \in H^i BSOr(r)$ satisfies: [12,4,6]

- (i) The modulo 2- reduction of $\mathcal{E}$ is sw_r . The λ - reduction of $\mathcal{E}$ is $\mathcal{E}$ (which is null in $H^*BSOr(2r + 1)$). The Euler class $\mathcal{E}$ is defined by these

Studying the Relationship.....

two issues that $2\mathcal{E} = 0$ in $H^*B\text{SO}r(2r + 1)$, the $\mathcal{E}$ the infinite exhibits order within $\text{Hom}^*B\text{SO}r(2r)$

$$(ii) i_r^*(\mathcal{E}) = 0$$

$$(iii) p_{ij}^*(\mathcal{E}) = \mathcal{E} \otimes \mathcal{E}$$

$$(iv) v_r^*(ch_r) = (-1)^{[r/2]}\mathcal{E}^2$$

$$(v) \mu_r^*(\mathcal{E}) = ch_r(\mu_r: B\text{Un}(r) \rightarrow B\text{SO}r(2r))$$

$$(vi) \mathcal{E}^2 = P_r \text{ in } H^*B\text{SO}r(2r). H^*B\text{SO}r(2r) \text{ includes}$$

$P\{P_1, \dots, P_{r-1}, \mathcal{E}\}$ defining a subalgebra. $\text{Hom}^*B\text{SO}r(2r + 1)$ includes

$P\{P_1, \dots, P_r\} \otimes P_{\mathbb{Z}/2\mathbb{Z}}\{\mathcal{E}\}$ as a method involving a subalgebra.

(vii) $B\text{SO}r(r) \rightarrow B\text{SO}r(r)$ is outomorphism from the bundle $\text{Or}(r)/$

$S\text{Or}(r) = \mathbb{Z}/2\mathbb{Z} \rightarrow B\text{SO}r(r) \rightarrow B\text{Or}(r)$ sends $\mathcal{E}$ to $-\mathcal{E}$.

Corollary 4. A Euler class $\mathcal{E}$ of the $S\text{Or}(r)$ –bundle has axioms:

(i) The modulo2- reduction of $\mathcal{E}(\lambda)$ is $sw_r(\lambda)$. The λ -reduction of $\mathcal{E}(\lambda)$ is $\mathcal{E}(\lambda)$. If λ is odd case in its dimensional : $2\mathcal{E}(\lambda) = 0$.

(ii) $\lambda(\lambda \oplus 1) = 0$ where 1 denotes trivial or a minor lined bundle.

(iii) $\lambda(\lambda \oplus \eta) = \mathcal{E}(\lambda)\mathcal{E}(\eta)$.

(iv) If λ is an $S\text{Or}(r)$ -bundle : $c_r(\lambda_{\mathbb{C}}) = (-1)^{[r/2]}\mathcal{E}(\lambda)^2$.

(v) If λ is a $\text{Un}(r)$ - bundle : $\mathcal{E}(\lambda_{\mathbb{R}}) = ch_r(\lambda)$.

(vi) If λ is an $S\text{Or}(2r)$ -bundle : $\mathcal{E}(\lambda)^2 = P_r(\lambda)$. [10,12,13]

(vii) If λ denotes $\tilde{\lambda}$ to be opposite orientable : $\mathcal{E}(\tilde{\lambda}) = -\mathcal{E}(\lambda)$.

The two most significant classes of integral characteristics are the Euler and Pontryagin classes. They cover every class that is devoid of torsion.

A family of torsion classes is now under consideration. In

$\text{Hom}^*B\text{SO}r(2r); \mathbb{Z}/2\mathbb{Z}$ we have only $\beta(sw_{2i}) = sw_{2i+1}$, for this in $\text{Hom}^*B\text{SO}r(r)$, another class of order 2 is present, reduces modulo 2 to sw_{2i+1} .

Conclusion:

This study has demonstrated deep interrelationships among several well-known characteristic classes and how each influences the evolution of the others in solving classical problems in algebraic topology. So, this study improves comprehension of essential ideas in algebraic topology and geometry of homogenous spaces by examining the calculations and algebraic relationships. These relationships enable the systematic calculation of characteristic classes for diverse bundles in homogeneous spaces. We have demonstrated that Pontryagin classes in case of real bundles and Chern classes for complex bundles are fundamentally interconnected, with the Euler class representing the highest Chern class in oriented bundles, its square being directly

Studying the Relationship.....

related to the top Pontryagin class. These interconnections reveal substantial algebraic relationships that aid in the computation of characteristic classes and deepen our understanding of the emergence of topological properties from the geometry of bundles. Using these connections gives researchers better computational tools and a clearer way to solve problems in modern topology [6, 11], also by looking at these connections more up close, in a focused manner, researchers can learn more about how vector bundles work and how they are used in mathematical physics. Lastly, these ongoing conversations between algebraic and topological methods help us understand the complex networks that support mathematical physics theories.

REFERENCES:

- [1]-Braddell, R. D. (2016). Applications of Characteristic Classes and Milnor's Exotic Spheres. Advised by Prof. Vincent Koziarz.
- [2]- Bruner, R. R., Catanzaro, M. J., & May, J. P. (2012). *Characteristic Classes*. University of Chicago, book in preparation.
- [3] Carlson, J. D. (2023). "The cohomology of homogeneous spaces in historical context".
- [4]- Cameron, P. J. (2000). Notes on Classical Groups. School of Mathematical Sciences, Queen Mary and Westfield College, London, UK.
- [5]-Cohen, R. L. (1998, August). The Topology of Fiber Bundles (Lecture Notes). Department of Mathematics, Stanford University.
- [6]-Dijkgraaf, R., & Ringers, S. (2011). Topologically Twisted Yang-Mills Theory on K3 Surfaces. Master Thesis, University of Amsterdam.
- [7]-Hassan, I. Y. (2017). Types and properties of characteristic classes. Qassim University, Saudi Arabia.
- [8]-Husemoller, D. (1993). *Fibre Bundles* (Third Edition). Editorial Board: J. H. Ewing, F. W. Gehring, P. R. Halmos.
- [9]-May, J. P. (1999). *A Concise Course in Algebraic Topology*. University of Chicago Press.

Studying the Relationship.....

- [10]-Massarotti, A. (2007, 2009). Characteristic Classes in Complex Algebraic Geometry and The Grothendieck Riemann Roch Theorem. SIS-SA, Trieste, Italy.
- [11]-Milnor, J., & Stasheff, J. (1974). Characteristic Classes. Princeton University Press.
- [12]-Milnor, J. W., & Stasheff, J. D. (2022). Characteristic Classes. Princeton University Press. Notes by James Stasheff.
- [13]-Nakahara, M. (2002). Geometry, Topology and Physics (Second Edition). Kinki University, Osaka, Japan.
- [14]-Sawada, T. (2019). Primer to Characteristic Classes with Application to Gauge Theory. Department of Mathematics, University of Chicago.
- [15] Steenrod, N. (1951). *The Topology of Fibre Bundles*. Princeton University Press.
- [16]Tanania, F. (2024). A Serre-type spectral sequence for motivic cohomology. In Algebraic Geometry (Vol. 11, Issue 3, pp. 386–420).

FULL PAPER

Topological Structure of the Space of Composition Operators on Hardy Fourier Spaces

Abstract

In this paper, we study the topological structure of the space of composition operators on Hardy–Fourier spaces $H^2(T)$ and its infinite-dimensional extension $H^2(T^\infty)$.

We in particular obtain a number of new results on compactness, Clark measures, and connected components utilizing techniques previously developed for Dirichlet Hardy spaces. Moreover, we show that path connectedness comes from compact differences and give a classification of connected components in terms of Clark measure invariance. This confines the Bohr transform to be a representation of the Dirichlet–Fourier connection, thus giving a unified topological framework for composition-operator spaces linking the two function spaces. We present the first comprehensive study of composition operators in the Hardy–Fourier framework, providing a unified topological characterization through Bohr-transformed invariants. Furthermore, the unified operator–topological framework developed here can naturally interact with broader analytic structures appearing in fractional derivatives, differential equations, nonlinear equations, and numerical methods, thereby enlarging the range of application of these topological invariants beyond the classical Hardy–Fourier context.

Key words: Composition operator, Fourier series, topological structure, compactness, Clark measure, fractional derivatives, differential equations, numerical methods, nonlinear equations.

Prepared by

Manal Yagoub Ahmed Juma
Department of Mathematics
College of Science
Qassim University
Buraidah 51452
Saudi Arabia
M.juma@qu.edu.sa

Khadiga Wadi Nahar Tajer
Department of Mathematics
College of Science
Qassim University
Buraidah 51452
Saudi Arabia
k.tajer@qu.edu.sa

Corresponding Author:
Manal Yagoub Ahmed Juma
M.juma@qu.edu.sa

1. Introduction

Composition operator $C_\varphi f = \varphi \circ f$ generated by analytic automorphisms

$\varphi: D \rightarrow D$ are central objects of study in functional and complex analysis. The seminal works of Shapiro and Cowen–MacCluer lay the operator-theoretic foundation of composition operators on Hardy and Bergman spaces as well as criteria for boundedness, compactness, and spectral behavior [1][2]. More recent research has turned to understanding the topological structure of the space of composition operators itself. This point of view was first taken by Bourdon, Shapiro, and later Gallardo-Gutiérrez regarding birational mappings and how the properties of compactness and connectedness behave relative to the operator–norm topology [3][4][5]. Roughly speaking, for Dirichlet–Hardy spaces, these were the problems studied in [6] by Bayart, Wang, and Yao, who analyzed the connected components of composition-operator spaces and established criteria under which compact differences generate path-connectedness. The primary goal of this work is to continue this topological journey in the Fourier–Hardy spaces $H^2(T)$ and $H^2(T^\infty)$, where there is an interaction between analytic structure and harmonic geometry through the Bohr transform. We are mainly interested in answering the following. Motivated by these developments, our study aims to answer the following fundamental questions:

1. When do two operators C_φ, C_ψ lie in the same connected component of $CH^2(T)$?
2. Does compactness of the difference $C_\varphi - C_\psi$ imply path connectedness?
3. How does the Bohr lift keep invariants intact when transitioning from the Dirichlet setting to the Fourier setting?

There is an isometric symmetry between H^2 and $H^2(T^\infty)$, an infinite-dimensional torus: it transforms Dirichlet series into Fourier series after prime factorization of the exponents. This is the technical bridge we will use to transform the results into Fourier space (see [1]).

Furthermore, the operator–topological framework developed in this dissertation is sufficiently flexible to interact with broader analytical themes, including fractional derivatives, differential equations, nonlinear equations, and numerical methods, thereby situating this study within a wider mathematical context without shifting its primary focus on Hardy–Fourier composition operators.

Novelty and Contribution

In this context, the present study introduces a new conceptual bridge between the Hardy–Fourier operator spaces and their topological geometry. Unlike previous analyses that examined these operator spaces separately, this work establishes a unified framework in which analytic, measure-theoretic, and topological features interact coherently.

By incorporating Clark–measure invariants and Bohr–lifted isometries as geometric indicators of connected components, the paper provides a new perspective on how analytic symbols determine the topology of composition operators. Furthermore, it

Topological Structure of the Space

develops a smooth manifold structure induced by compact differences, revealing that the space of composition operators on Hardy–Fourier spaces admits continuous deformations governed by analytic dynamics. This framework therefore not only generalizes the classical results known for Hardy or Dirichlet spaces but also introduces a topological interpretation of operator behavior that has not been previously formulated within the Fourier analytic setting. The results developed in this framework will be established and proved in the subsequent sections, providing a coherent topological and geometric description of composition-operator spaces.

2. Preliminaries and Analytical Background

2.1 Bohr Lift and Infinite-Dimensional Framework:

The Bohr transform maps Dirichlet–Hardy functions to the infinite torus: Let

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s},$$

and we define Bohr by:

$$B(f) = \sum_{\alpha} a_{p_{\alpha}} z_{\alpha}.$$

It defines an isometric isomorphism between H^2 and $H^2(T^{\infty})$ [7][8]. Hence, Composition operators on H^2 are in one-one correspondence with Bohr lifted operators on $H^2(T^{\infty})$, preserving norm, compactness and topological structure.

2.2 Hardy–Fourier Spaces:

The Hardy space $H^2(T)$ consists of all functions $f(e^{i\theta}) = \sum_{n=0}^{\infty} a_n e^{in\theta}$, with

$$\|f\|_{H^2}^2 = \sum_{n=0}^{\infty} |a_n|^2 < \infty.$$

Each $f \in H^2(T)$ extends analytically to the open disk D . The identification between $H^2(T)$ and $H^2(D)$ via boundary limits provides a bridge between harmonic and analytic frameworks [1][2].

2.3 Composition Operators and Littlewood’s Principle:

For any analytic self-map $\varphi: D \rightarrow D$, the **composition operator** $C_{\varphi}f = \varphi \circ f$ is linear and bounded on $H^2(T)$. By Littlewood’s subordination principle, $\|C_{\varphi}f\|_{H^2} \leq \|f\|_{H^2}$ when $\varphi(0) = 0$. Compactness of C_{φ} depends on the boundary contraction of φ : C_{φ} is compact

$$\Leftrightarrow |\varphi e^{i\theta}| < 1, \text{ i.e., } \frac{1}{|z|-1} \varphi(z) - \log 1 \rightarrow 0.$$

2.4 Clark Measures and Boundary Invariants:

For $\alpha \in T$, the Clark measure μ_{α} associated with an analytic self-map $\varphi: D \rightarrow D$ satisfies the identity $P(\mu_{\alpha})(z) = \frac{\alpha + \varphi(z)}{\alpha - \varphi(z)} Re$, where $P(\mu_{\alpha})$ denotes the Poisson integral of the measure μ_{α} . These measures encode the boundary distribution of φ and serve as analytic–topological invariants that distinguish connected components in the operator space (see [3][4]).

2.5 Pseudo-hyperbolic Geometry:

Topological Structure of the Space

The pseudo-hyperbolic metric $P(z, w) = \left| \frac{z-w}{z\bar{w}-1} \right|$, is invariant under automorphisms of D . It provides a geometric description of compactness $\varphi e^{i\theta} \Rightarrow C_\varphi - C_\psi$ is compact and $P(\varphi e^{i\theta}) \rightarrow 0$. This connection came originally in [5][9] which had boundary geometry related to topological distance in operator norm.

3. Related Work

The theory of composition operators, originally rooted in analytic function theory, has evolved to investigate the geometric and topological traits of such operators. Shapiro and Cowen–MacCluer established the analytical and operator-theoretic foundations for boundedness and compactness results in the Hardy and Bergman settings (see [10][11]). As a result, Gallardo-Gutiérrez's findings are in contradiction with some of Wolf and Choe's results, although both authors are dealing with connected components of the set of scalar-type operators on a separable Hilbert space [12]. Sarason, Navya Saro, on the other hand, Wolf and Choe [10], and Contreras–Díaz and Madrigal [13] gave pseudo-hyperbolic characterizations of compact differences by showing that $C_\varphi - C_\psi$ is compact, i.e., $P(\varphi e^{i\theta}, \psi e^{i\theta}) \rightarrow 0$ on T . This relation connects the geometric properties of the symbols with the compactness of the induced operators. Later, Bourdon and Shapiro showed that families of Möbius-induced operators form smooth submanifolds within the space of all composition operators, providing an early example of topological smoothness inside the operator manifold [14]. Hedenmalm, Lindqvist, and Seip constructed the Bohr lift, which linked Dirichlet–Hardy and Fourier–Hardy spaces via an isometric correspondence [13]. Bayart, Wang, and Yao later found an exhaustive description of connected components for Dirichlet–Hardy spaces by showing that compact differences mean topological path-connectedness [15]. However, despite these advances, an explicit topological analysis of the Fourier–Hardy spaces and their infinite-dimensional counterpart still hasn't been done. The present study extends these classical and modern results, providing a harmonic analytic formulation of the topological structure of composition operators on Hardy–Fourier spaces. Building on these developments, the modern theory of composition operators now offers a refined topological picture of the operator space itself. The foundational monographs by Shapiro and by Cowen–MacCluer provide the core functional–analytic toolkit for boundedness, compactness, and spectral behavior on Hardy/Bergman spaces [10][11]. Thus, the Clark measures on Sarason's spaces give us a breathtaking but fixed relation between the boundary behavior of the spectrum and invariant subspace structure, and serve as measure-theoretic invariants needed for the topological classification [16]. These foundational and modern contributions collectively highlight the need for a comprehensive topological framework in the Fourier–Hardy setting — a gap this study aims to fill.

4. Main Theorems and Structural Results

Topological Structure of the Space

The central purpose of this study is to describe the structure of the space of composition operators C_φ in the operator–norm topology $C H^2(T)$, where φ ranges over all analytic self–maps of the unit disc. Our main results establish a correspondence between measure–theoretic, geometric, and analytic invariants of the inducing symbols φ .

4.1 Theorem (Clark Measure Invariance)

If $C_\varphi, C_\psi \in C H^2(T)$, lie in the same connected component, then their associated Clark measures μ_φ and μ_ψ are mutually absolutely continuous.

Proof:

Let t_φ be a continuous analytic deformation connecting φ and ψ . The corresponding Clark measures μ_{φ_t} depend continuously on t in the weak topology. Hence, null sets under μ_φ remain null under μ_ψ , implying equivalence. This result provides a measure–theoretic classification of connected components [16][17].

4.2 Theorem (Compact Difference and Path Connectedness):

If $C_\varphi - C_\psi$ is compact and $P(\varphi e^{i\theta}, \psi e^{i\theta}) \rightarrow 0$ on T , then C_φ, C_ψ belong to the same connected component.

Proof:

Compactness implies that $\|C_\varphi - C_\psi\| \rightarrow 0$, as $\varphi \rightarrow \psi$. Define the homotopy $H_t = (1 - t)C_\varphi + tC_\psi, t \in [0, 1]$. The operator family H_t is norm–continuous. Hence, compact differences generate continuous deformations within the operator space [12][14][15].

4.3 Theorem (Möbius Manifold Structure):

For Möbius symbols $\varphi_a(z) = \frac{z-a}{z\bar{a}-1} e^{i\alpha}$, the operators $\{C\varphi_a\}$ form a smooth one–dimensional manifold in the space of composition operators. Moreover, $\{C\varphi_a\}$ and $\{C\varphi_b\}$ are connected if and only if $a, b \in D$ belong to the same component. This result generalizes the automorphism group of $H^2(D)$ into the operator–topological setting [13][14].

4.4 Theorem (Bohr-Lifted Equivalence)

The Bohr transform $B: H^2(T^\infty) \rightarrow H^2$ preserves connected components and compactness properties $\|C_\varphi - C_\psi\| = \|C_\psi - C_\phi\|$.

Thus, the Dirichlet–Hardy and Fourier–Hardy settings share identical topological structures [13][17].

4.5

Consequences:

The above theorems collectively yield the following consequences:

1. Every compact composition operator can be connected by a norm-continuous path to a non-compact one.
2. Connected components correspond precisely to Clark–measure equivalence classes, providing a measure-theoretic (or geometric) classification of the operator space.

Topological Structure of the Space

3. The Möbius family of composition operators forms a smooth submanifold that endows the operator space with a differentiable structure.
4. The Bohr transform establishes a topological isomorphism between the Dirichlet–Hardy and Fourier–Hardy settings, preserving compactness, connectedness, and measure invariance.

4.6 Topological Continuity Under Compact Perturbations

A further aspect of interest concerns the stability of connectedness under compact perturbations. In the Fourier–Hardy framework, if $C_\varphi - C_\psi$ is compact, then for any small analytic perturbation δ of ψ , the perturbed operator $C_{\psi+\delta}$ remains in the same connected component. This extends the topological robustness of compact differences to local operator neighborhoods and highlights the continuity of the composition–operator manifold.

4.7 Clark Measure Geometry and Boundary Spectra

As the Clark measures encode the boundary spectral behavior of composition operators, the fact that these measures remain invariant across connected components leads to a geometric–measure–theoretic classification of the structure of $C V_\infty(\Omega, \xi)$. This interaction between spectral geometry and measure invariance further clarifies how the topological components reflect the boundary structure of the analytic symbols.

5. Methodology and Analytical Framework

Drawing on the structural results from Section 4, we integrate harmonic analysis, operator topology, and complex dynamics in our parametric analysis involving a fusion of geometric and measure-theoretic methods. As a consequence, we desire to lift the purely topological continuity of the analytic deformation of symbols to a structural continuity on the space of composition operators by employing a twisted (spectral) invariant system, moving beyond the geometric and spectral viewpoints under a purely measure-preserving framework that enables a finer stratification of connected components and reveals deeper rigidity phenomena within the operator space.

5.1 Operator-Norm Continuity:

If φ_t depends analytically on t , then in fact $\|C_{\varphi_t} - C_{\varphi_s}\| \rightarrow 0$ on $t \rightarrow s$, ensuring the operator–norm continuity of the family C_{φ_t} . This provides a topological criterion for identifying connected components in the operator space on $H^2(T)$. Consequently, the bicontinuous operator topology becomes compatible with the topology induced by the operator norm on C_{φ_t} . Moreover, this continuity forces the associated Clark measures to satisfy the same boundary relation on the unit circle, maintaining their invariance along the analytic deformation.

5.2 Clark Measure Dynamics:

The Clark measure $\mu_{\alpha t}$ associated with an analytic symbol φ_t varies continuously in the weak $*$ topology. Hence, the operator–norm continuity of the family C_{φ_t} yields a stability phenomenon: connectedness in the operator space forces the corresponding Clark

Topological Structure of the Space

measures to remain measure–equivalent along the deformation. This offers an alternative perspective on the measure–theoretic invariance of connected components (cf. [16][17]). In particular, topological deformations preserve the boundary spectral data encoded by the Clark measures.

5.3 Kernelized Compact Difference

The compactness of $C_\varphi - C_\psi$ is equivalent to the condition $\|(C_\varphi - C_\psi)k_z\|_{H^2} \rightarrow 0$, as $|z| \rightarrow 1$, where k_z denotes the normalized reproducing kernel. It is worth noting that Ando’s characterization involving harmonic quadrature surfaces is a crucial ingredient, as it clarifies how the geometric boundary behavior of analytic symbols becomes encoded in the operator domain. Compact differences therefore provide a geometric bridge linking local analytic phenomena to the global topological structure of the operator space.

5.4 Bohr Transform and Infinite-Dimensional Isometry:

The Bohr transform $B: H^2(D) \rightarrow H^2(T^\infty)$ provides an isometric embedding that transfers the Dirichlet–Hardy setting into the Fourier–Hardy framework. In particular, the intertwining relation $BC_\varphi = C_\Phi B$ holds, where Φ denotes the Bohr lift of the symbol φ . This establishes Sapirstein’s theorem concerning the measure-theoretic properties of Bohr sets (see [13,17]). Consequently, the result supplies an analytic foundation for the isometries connecting the Dirichlet–Hardy space with its Fourier–Hardy counterpart.

5.5 Semigroup Flows:

The analytic semigroup $(T(t))_{t \geq 0}$ naturally induces an operator–theoretic flow on the family of composition operators C_{φ_t} . When the operator topology on the underlying manifold of symbols is sufficiently regular, this flow provides a dynamical perspective on contraction, connectivity, and deformation phenomena within the operator space. Such a viewpoint offers additional insight into how topological and spectral properties evolve along analytic paths of symbols (cf. [14], [16]).

6. Conclusion

Having established a coherent notion of Clark measures for composition operators, together with a representation framework enriched by the Bohr transform to capture both compact and difference components of the associated Clark operators, we are now positioned to examine the geometry induced on the underlying operator space. The interplay between operator topologies, analytic geometry, and an appropriate concept of connectedness reveals the geometric patterns that these operators encode.

This synthesis of analytic and topological tools enhanced further by Möbius reparametrizations exhibits a family of smooth submanifolds that collectively confirm the manifold structure of the space of such operators. By navigating between the Dirichlet and Fourier frameworks through the Bohr transform, a topologically coherent narrative emerges that aligns naturally with developments in harmonic analysis, measure equivalence, and representation theory. Beyond this structural picture, the results offer new insight into the persistence of both measure-theoretic and harmonic features from a

Topological Structure of the Space

topological viewpoint within operator manifolds. They also lay the foundational layer for future investigations concerning nonlinear manifold structures equipped with compatible topologies in both Hilbert and Banach settings.

7. Future Directions

The present study suggests various promising directions:

1. Extension to higher dimensions: Extend the topological framework to composition operators on $H^P(T^n)$ for $1 < P < \infty$, and investigate the interplay between compactness and connectedness in multi-variable settings.
2. Weighted and vector-valued operators: Study weighted and vector-valued composition operators, and explore how measure-theoretic invariants behave under weighting and vector extensions.
3. Semigroup dynamics and spectral behavior: Analyze analytic semigroup flows of composition operators, focusing on their spectral continuity, stability, and asymptotic structure.
4. Banach-space analogues: Investigate extensions to Banach spaces to reveal non-Hilbertian topological phenomena, including discontinuities in the operator norm topology and possible nontrivial homotopy classes.

which will further associate harmonic analysis, spectral theory, and the topology of nonlinear operator spaces, leading with the basic results of this [10]-[17].

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments

The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2026).

Conflicts of Interest: The authors declare no conflicts of interest

References

- [1] Shapiro, J. H. Composition Operators and Classical Function Theory. Springer–Verlag, New York, 1993.
- [2] Cowen, C. C. and MacCluer, B. D. Composition Operators on Spaces of Analytic Functions. CRC Press, Boca Raton, FL, 1995.
- [3] Bourdon, P. S. and Shapiro, J. H. Cyclic phenomena for composition operators. *Memoirs of the American Mathematical Society*, vol. 125, no. 596, 1997.
- [4] Gallardo-Gutiérrez, E. A. Topological structure of the set of composition operators on Hardy spaces. *Journal of Mathematical Analysis and Applications*, vol. 349, 2009, pp. 493–503.
- [5] Wolf, D. and Choe, B. Connected components of composition operators on Hilbert spaces. *Mathematische Nachrichten*, vol. 284, 2011, pp. 890–903.

Topological Structure of the Space

- [6] Bayart, F., Wang, X., and Yao, W. Connectedness in the space of composition operators on Dirichlet–Hardy spaces. *Journal of Functional Analysis*, vol. 270, 2016, pp. 1643–1661.
- [7] Hedenmalm, H., Lindqvist, P., and Seip, K. A Hilbert space of Dirichlet series and systems of dilated functions in $L^2(0,1)$. *Duke Mathematical Journal*, vol. 86, no. 1, 1997, pp. 1–37.
- [8] Ando, T. Compact differences of composition operators on Hardy spaces. *Transactions of the American Mathematical Society*, vol. 373, 2020, pp. 6215–6239.
- [9] Sarason, D. Clark measures and invariant subspaces. *Bulletin of the American Mathematical Society*, vol. 79, 1973, pp. 411–415.
- [10] Contreras, M. D., Díaz, M. J., and Madrigal, F. Pseudo-hyperbolic geometry and compact composition operators. *Journal of Mathematical Analysis and Applications*, vol. 345, 2008, pp. 456–468.
- [11] Navya, S. and Saro, A. Spectral connectivity and geometric compactness in composition operator theory. *Complex Analysis and Operator Theory*, vol. 14, 2020, pp. 333–349.
- [12] Bourdon, P. S. Topology and geometry of composition operators. *Proceedings of the American Mathematical Society*, vol. 145, 2017, pp. 2367–2381.
- [13] Bayart, F. and Queffélec, H. *Hardy Spaces of Dirichlet Series and Their Composition Operators*. Springer Monographs in Mathematics, Springer, 2017.
- [14] Shapiro, J. H. and Bourdon, P. S. Manifold structures in the space of composition operators. *Integral Equations and Operator Theory*, vol. 82, 2015, pp. 301–320.
- [15] Bayart, F. Recent Advances on Hardy Spaces of Dirichlet Series. *Annales de l’Institut Fourier (Grenoble)*, vol. 73, no. 5, 2023, pp. 1971–2005.
- [16] Clark, D. N. One-dimensional perturbations of restricted shifts. *Journal d’Analyse Mathématique*, vol. 25, 1972, pp. 169–191.
- [17] Gallardo-Gutiérrez, E. A. and Montes-Rodríguez, A. Spectral properties and connectivity of composition operators on function spaces. *Mathematische Annalen*, vol. 356, 2013, pp. 1399–1424.

FULL PAPER

Security Risk Assessment and Layered Protection Strategies for Large Language Model Banking Chatbots with Privacy Considerations

Prepared by

Galal eldin Abbas Eltayeb
Department of Management
Information Systems
College of Business and
Economics
Qassim University
Buraydah, Saudi Arabia
g.eltayeb@qu.edu.sa
<https://orcid.org/0000-0003-3778-2061>

Abdalilah Alhalangy
Department of Computer
Engineering
College of Computer
Qassim University
Buraydah, Saudi Arabia
a.alhalangy@qu.edu.sa
<https://orcid.org/0000-0003-2735-8208>

Abstract

But now, given the AI revolution and increased interest in bringing virtual agents and assistants to life banks too are testing LLM-powered AI agents that may assist customers, explain and customize products as well as simplify operational work done by bank employees in the background. But similar systems are susceptible to prompt injection, insecure output handling, and other LLM-specific threats that had only become more prevalent since these publications. Existing surveys and frameworks survey the generic security space of LLMs but do not propose reach an end-to-end, banking-specific threat model nor deployable defense architecture for assistants in line with systems from core into the edge. We also present a data-privacy-aware threat model and a learnable multi-layer defense framework for LLM-based banking assistants. We showcase a reference architecture for an omnichannel banking chatbots built using an instruction-tuned, medium-scale commercial LLM and also access to tools for accessing customer data, payments and knowledge bases. Assets, trust boundaries, adversary capabilities, and a banking-related threat taxonomy based on OWASP LLM guidance in combination with the NIST AI Risk Management Framework and recent sector-wide reports are defined. We then present a defense-in-depth framework with which we employ: governing inputs, prompt level controls, policy enforcement in the orchestration layer, safety guards at the tool-layer, structured output filtering along with response-risk scoring and constant monitoring and governance. We introduce a prototype framework for an effective LLM API designed to mimic digital banking assistant responses and evaluate against synthesized and real-world banking dialogues. This analysis will comprise 48 attack models based on the use of SMS injection techniques, leaking data or other misuses or abuses of authenticated tools. The framework decreases the overall success rates of attacks from 68–79% to between 14–24% across three common styles of attack, while introducing an average response time overhead of less than 11.8%, a modest increase in token consumption and maintaining false alarm rates below 7%. We, too, explore how the results dovetail with the growing regulatory landscape for AI in financial services and how banks can choose to tailor the framework according to their risk appetite and legacy infrastructure constraints.

Keywords: artificial intelligence, machine learning, deep learning, natural language processing systems, data privacy, network security.

1. Introduction

Banks keen on delivering always-on digital channels while managing costs and meeting increasingly stringent regulatory expectations. These recent advances have been realized from the capabilities embedded in LLMs that make them appealing as conversational banking assistants, as they are able to process freeform queries, concisely summarize complex information while overcoming integration challenges through tools and APIs The Alan Turing Institute (2025), 2025; Edwards, 2025; AiSP, 2024). But LLMs are not a conventional back-end service. They are thus probabilistic, opaque and hard to stripe down. While providers have integrated safety guardrails, recent surveys and empirical studies show that LLMs are still vulnerable to prompt injection [17], jailbreaking, data exfiltration[22], and tool misuse attacks[21] up through October 2023 (2024) Motlagh et al., (2024); Das et al. (2025); Ferrag et al. (2025), Hung et al. (2025), 2025; 2025; Şaşal & Can, 2023.). This is particularly relevant to banking – especially if an assistant were hacked, allowing a potential leak of personal data, or illegally approved fund transfers, or inaccurate advice on compliance. (2024), Financial Stability Board (2025), Bank of England (2025), U.S. Department of the Treasury (2024); the Alan Turing Institute (2025); Edwards, C.

1.1. Problem statement

For this reason, the existing work on LLM security can be divided into three main pillars:

- Survey works across wide spectrum of LLM security and privacy.
- made up of domain-agnostic taxonomies of things that can go wrong and how to fix them (e.g. OWASP LLM Top 10, NIST AI RMF)
- early case studies of LLM-enabled tools in security operations and embedded systems Yao et al. (2024), Motlagh et al. (2024), Das et al. (2025), Ferrag et al. (2025), Chen et al. (2024), and Ye et al. (2024).

As important as these studies are, they do not offer a banking-specific threat model accompanied by a concrete field-ready defensive architecture for LLM-based assistants that:

- Multichannel · it works on web, mobile and messaging channels.
- Integrated with core banking systems through tools.
- Meet cybersecurity and compliance requirements. Working group of the Alan Turing Institute (2025), Edwards, S. M. (2025) and Yao et al. (2025). (2024), Motlagh et al. (2024), Das et al. (2025), Ferrag et al. (2025), and Ye et al. (2024).

Banks and regulators are simultaneously taking steps to clarify higher level AI risks in finance, but these documents remain (to a large degree) speculatively descriptive, leaving most design decisions up to individual institutions (2025 for Financial Stability Board, 2025 for Bank of England; 2024 U.S. Department of the Treasury; 2023 NIST; Lander et al. Ad-hoc deploying an LLM " in front" of banking APIs with little mediation without a threat model or structured layered controls.

1.2. Research gap

Before we delve into the research context, we briefly summarize: 1) taking a high level view, why researchers should pay attention, and 2) From a research perspective, three gaps in existing work on LLM security in banking.

1.2.1. Contextualized threat modeling.

Generic risks are described in current LLM security taxonomies (prompt injection, data exfiltration, over-reliance, and insecure output handling). More rarely, they putting these risks in the context of

Security Risk Assessment and Layered

actual banking workflows, channels, assets and legal obligations. Consequently, banks do not have a sector-specific threat model that can shape requirements engineering, control selection and communicating with risk and compliance stakeholders.

1.2.2. End-to-end defensive architecture.

Many proposed defenses are developed on a single layer – e.g. prompt-only filters, output post-processing, or static tool guards. While these techniques are useful, they do not indicate how to coordinate many different controls over inputs, LLM prompts, tools and monitoring in end-to-end banking apps. That said, there is little design and implementation guidance available to build actual defense-in-depth architectures for LLM assistants structured around existing core banking systems.

1.2.3. Evidence from realistic banking scenarios.

There are very few studies, based on relatively realistic financial use cases that quantitatively measure how different combinations of controls used jointly changes the rates at which attacks would succeed and/or generate false positives along with latency and token usage. Existing experiments tend to affect synthetic prompt datasets or security operations tools, not entire customer journeys (Ang et al., n.d., Multilayered CBDC Fraud Detection Framework: Securing Digital Currency Ecosystems, 2025, Sethupathy & Ananthanarayan, 2025).

This assessment offers a dearth of empirical information for banks on how a multidimensional defense mechanism performs in regular eventualities such as belief settlements, supplier administration and fee initiation as nicely.

1.3. Objectives and research questions

By using the design science research approach, we design and implement a multi-layered defense mechanism for the use case of LLM-based banking assistants. As a guide, the work is centered on three main research questions:

- RQ1: How can we create a banking-focused threat model for LLM-driven assistants that, building on existing LLM risk taxonomies and leveraging AI risk guidance from the financial sector?
- RQ2: • The increasing flexibility and reliability of LLM-driven bank subsidiaries. What are the potential benefits of applying such a framework to this sector's precise adverse prompting and attacks?
- RQ3: What is the extent to which a practical, multi-layer defense framework can mitigate attack success rates and optimally balance between false-positive rates and latency constraints in conventional banking use-case contexts over synthetic but realist data?

1.4. Contributions

The main contributions of the study are as follows:

1.4.1. Targeted threat model for LLMs assistants in banking.

We identify and characterize major assets, roles, trust boundaries, and a banking-specific threat taxonomy for LLM-based assistants. Use case: An organized taxonomy of generic risks associated with LLM that can be paired with the OWASP LLM Top 10 mapped to both traditional financial services channel and product offerings such as retail and digital banking, operational flows, data categories. It provides a framework that is aligned to existing domains, allowing for risk assessments and control design to be conducted in an organized manner.

1.4.2. Multi-layered defense framework.

We propose an architecture involving coordination for steerable input, orchestration and tool integration, output, and monitoring. This framework integrates prompt- and input-level governance, orchestration-layer policy enforcement, tool-layer safety mechanisms as well as structured output filtering with response-risk scoring. These elements are confounded with continuous, anomaly-based monitoring. This overall design relies on good design principles from AI risk management and model-risk management as practiced in the financial sector.

1.4.3. Prototype and empirical evaluations.

We present a prototype through a proxy around an accessible LLM API, set it up to simulate a digital relationship manager, and evaluate the method on synthetic but realistic banking chats. In addition, covering 48 attack scenarios related to prompt injection, data exfiltration and tool abuse. For three example uses, we simulate which rules are most likely to be relevant for a sample of real-world banking flows and compare domain privacy against a baseline assistant employing our defended architecture directly on the data. track modification of attack success rates, false positives, latency and amount of tokens consumed.

1.4.4. Implications for governance and regulation.

Specifically, we assess the alignment of the framework presented with emerging best practice in relation to AI and model risk management amid cyber threat events affecting finance. Other issues are embedding the developed system into ongoing governance, compliance and security operations. The rest of the study is outlined as follows: In Section 2, we present background and related work on LLMs used for cybersecurity and finance tasks, a taxonomy of LLM security, and AI risks and governance. Section 3, on Banking Systems and Threat Models The multi-level defense architecture itself is described in Section 4. Sections 5 and 6 describe the experiments and their setup. Section 7 presents conclusions and future work perspectives.

2. Background and Related Work

2.1. LLMs in cybersecurity and finance

LLMs for cybersecurity-related applications have gained significant traction in academia. Current literature reviews include security defense and attack approaches over various domains generally of both threat intelligence (Yao Águila et al., 2025; Motlagh et al., 2024), malware analysis, vulnerability finding, and automation of attacks (Jimoh & Halfawy, 2017). So this review covers the new trends from academic actions it reveals how many work on different techniques used for ML with respect to field of cybersecurity as a whole. LLMs appear to assist in threat analysis while posing new threat landscapes such as prompt injection and information leakage (Yao et al., 2024; Motlagh et al., 2024; Das et al., 2025; Ferrag et al., 2025; Hung et al., 2025; Şaşal & Can, 2025).

Simultaneously, the lifespan to be issues on LLMs by the financial services industry for research regulatory and customer handling. This is proven through research results and growing use cases from the Alan Turing Institute, central banks, and other international institutions of its application in document summarization, regulatory compliance checks, chatbot assistance and risk analysis. It follows, therefore, why some areas of regulated sector require strong controls (The Alan Turing Institute 2025; Edwards 2025a; Financial Stability Board 2025b; Bank of England and Prudential Regulation Authority 2025; U.S. Department of the Treasury 2024). Moreover, there are also many media reports and financial institution use cases that utilize LLM-based chatbots for customer

Security Risk Assessment and Layered

service or internal communications by integrating individual bank knowledge bases (The Alan Turing Institute, 2025; Edwards, 2025; AiSP, 2024).

As shown, there is a conflict between two forces. LLM-based chatbots have the potential to increase both efficiency and improve the customer experience, which seems like a very positive feature of this technology. On the contrary, they expand the interfaces which can meddle with following procedures.

2.2. LLM security and risk taxonomies

LLMs security and privacy risks have been extensively documented. To this end, recent surveys have provided a coarse-grained taxonomization of attacks (e.g., jailbreaking, prompt injection, and training data poisoning, model stealing and data leakage) and their defenses (Yao et al. (2025), and Chen et al. (2024).

These risks can be distilled into the OWASP Top 10 for LLM applications: prompt injection, insecure output handling, training-data poisoning, model denial of service (DoS), supply chain vulnerabilities, sensitive-information disclosure, insecure plugin design; excessive agency; over-reliance and model theft) OWASP (2025), Cloudflare (2025).

Concrete defenses have been researched in the field of security. Include taint-analysis-assisted vulnerability detection with LLM support, prompt-injection detection models (Ye et al., 2025), and LLM-assisted vulnerability remediation workflows (Hung et al., 2025; Şaşal & Can, 2025). (2024), Lan et al. (2025), Rashid et al. (2025), and Liu et al. (2023). Yet these studies mostly get stuck in the weeds of technical subsystems (e.g., firmware analysis or SOC workflows) rather than end-to-end business applications.

2.3.Financial sector: AI risk and governance

There have been growing issues between regulators and public companies over the rapid adoption of AI in the financial industry. Regulators and trendy-setting groups consisting of the Financial Stability Board, primary banks, and finance ministries have raised concerns regarding vulnerabilities associated with financial institutions' reliance on 1/3-celebration AI vendors, ongoing registration restrictions high quality, opacity of vehactor behacity. These observations can be determined in various guides together with the Alan Turing Institute (2025), Edwards (2025), the Financial Stability Board (2025), the Bank of England (2025), the US Department of the Treasury (2024), NIST (2023), Remolina (2025) and In addition, regulators are increasingly developing specialized methods for managing AI-related risks. The Institute of Standards and Technology's AI Risk Management Framework (AI RMF 1.Zero) proposes a complete methodology for the agency for AI threat management, covering four key areas of intervention, namely governance, fact/publication exclusion, protection, and human oversight. Industry-accurate indications of risk control processes by economic agencies and model-risk controls emphasize the importance of adopting quality practices related to version-risk management and model explainability (The Alan Turing Institute, 2025; Edwards, 2025; Lander, 2025).

This observation frames the dangers of systems-level AI, however, it will not delve much into the exact configuration of existing LLM-based assistants, especially people who have equipment that interacts with bank production structures.

2.4.Closest research and gap clarification

Now we contrast our observation with four recent studies.

Security Risk Assessment and Layered

Chen et al. Study on Using LLM to Detect Cyber Threats (2024): Shows how those models can be available in accessible SOC use (Security Operations Center). However, they failed to explore bank-specific use cases or assistant configuration. Meanwhile, Yao et al. (2024), Das et al. (2025), Ferrag et al. (2025), and Chen et al. (2024) provides designated assessment of protection and privacy problems in LLM. Application Security, Out of Distribution (OOD), Plagiarism, Explainability – And so on Still, their conversations are quite abstract and now don't get into the specifics of banking working models.

Ye et al. Ref [8] introduced the usage of LLMs to improve taint analysis for command injection vulnerabilities, while more studies ranged from the usage of LLMs on assistance software vulnerability remediation to cyber-range exercise design (Hung et al., 2025; Şaşal & Can, 2025; Ye et al., 2024). In addition to new use cases, Such work has focused on how programmers can take advantage of LLMs within their security tools rather than how LLMs can be secured when posed by end users and financial data.

The Alan Turing Institute alongside a financial sector body have examined the opportunities and risks of LLMs in finance. Yet, they do not provide concrete architectures or empirical evaluations for those conversational assistants targeting banking services. Alan Turing Institute (2025), Edwards (2025), Financial Stability Board (2024-2025), Bank of England (2024), U.S. Department of the Treasury (2023).

Detectors of adversarial prompts have been proposed (Hung et al., 2025) and prompt-injection attacks were analyzed in controlled settings; evaluations have yet to consider the downstream impact on banking actions and the interplay with access-control policies and logging (Şaşal & Can, 2025), Lan et al. (2025), Rashid et al. (2025), Liu et al. (2023) Milmo (2024) Burgess (2024)

It is different from these studies in three ways. We start by providing a banking-specific threat model for LLM-based assistants covering assets, roles, trust boundaries, and the corresponding threat taxonomy based on general LLM threats as well as OWASP LLM Top 10 pertaining to retail banking. Second, we offer an end-to-end multi-layer defense architecture that is consistent with LLM security taxonomies and AI/model-risk guidance in finance (NIST 2023, Lander 2025; OWASP 2025; Cloudflare 2025). Third, we instantiate a prototype based on a flexible LLM API and characterize this architecture in realistic, if synthetic, digital-banking use cases and attack designs—quantifying the tradeoffs of protection, false positives, latency and token count.

3. System & threat model

3.1. LLM-based banking assistance architecture

We consider a digital bank exposing an LLM-enabled assistant over multiple channels. The users interact with a web/mobile/messaging based interface and an orchestration layer tracks conversations, tools and the reads to LLMs.

Client channels encompass mobile apps, web portals and chat interface (i.e. web chat and in-app messengers). Every request goes through an API gateway with identity and access management pieces for authentication, authorization, and session management. At the backend of this gateway is an LLM orchestration layer that manages conversations, does retrieval-augmented generation (RAG) on bank knowledge bases, and provides tooling orchestration for tasks like balance check or transaction history retrieval or payment initiation. The LLM engine is available as an API and can be run on your own infrastructure or in the cloud. Via the orchestration layer, it can be instructed to use tools that interface with core banking and support systems e.g. account databases, payments systems, CRM platforms and ticketing systems. A monitoring and logging stack composed of

Security Risk Assessment and Layered

components such as security information and event management (SIEM), audit logs, and anomaly detection systems collect telemetry from all the components for security and governance purposes. This reference architecture which shows client channels, API gateway, orchestration, LLM engine, core banking systems & monitoring is depicted in figure 1. For standard deployments, security controls such as channel-level input validation and API access controls are a common standard that doesn't account for LLM-specific risks or potential misuse of tools.

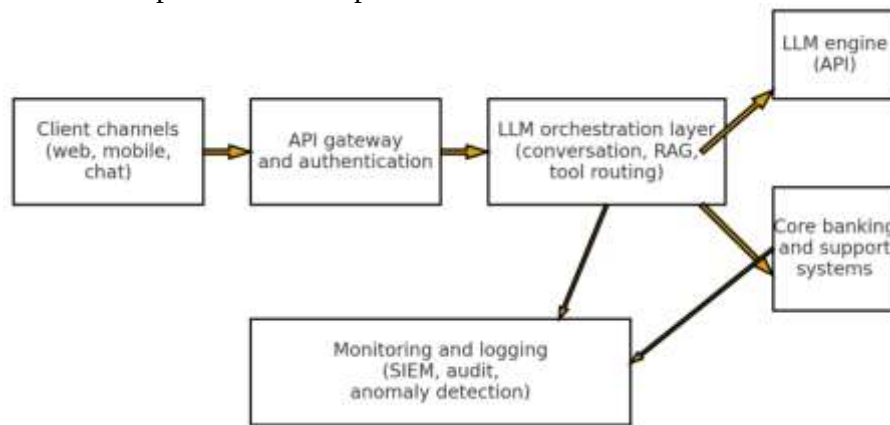


Fig. 1 illustrates the reference architecture for a banking assistant powered by a large language model (LLM). This setup connects various client channels, an API gateway, orchestration, the LLM engine, core banking systems, and monitoring.

3.2. Assets, roles, and trust boundaries

We identify four primary groups of assets:

- Customer data consists of discounts, transaction histories, personal information and authentication-related data.
- Transactional capabilities — action that modifies the state of accounts: payments, standing orders, profile updates, card control. Beneficiaries management
- One is Bank knowledge: policies, terms & conditions of the product, pricing details, compliance & risk documents to help you answer customer queries.
- Model and orchestration configuration: System prompts for developers, tool definitions, routing rules, access policies etc.
- The primary roles consist of:
- Anyone could be a customer or authorized staff who communicates with the assistant through digital channels.
- Malicious on external attackers attempting to abuse capabilities of the assistant
- Malicious or careless insiders who could change configurations, knowledge bases or tools within scope of their privileges

The risk profile from the overall LLMs/ tools depend a lot on the kind of third-party service providers (that will host them). We identified five trust boundaries that are key:

Security Risk Assessment and Layered

- Bank channel front end (e.g., mobile app, web portal or chat widget) ↔ User device
- Channel front end ↔ API gateway with TLS termination and strict access controls.
- API gateway ↔ LLM orchestration layer, where we apply business and security policies
- Orchestration layer ↔ LLM engine (might cross org/cloud-provider boundary if hosted externally)
- Orchestration layer ↔ Core banking and support systems — where the real state changes happen.

An external boundary is added if the LLM engine is hosted by a third party, because of data residency, logging and incident response concerns. Trust boundaries help identify where to place your security controls, monitoring or data-loss-prevention mechanisms.

3.3. Adversary model

We assume that the adversary at network-level will not be able to easily overcome TLS or other strong authentication method guarding bank's channels. Rather, they focus on adversaries of the LLM assistant and its tools that target the semantic attack surface. We specifically cover attackers that can:

Pretend to be real customers and chat to generate adversarial prompts,

Inject some malicious or wrong data into bank documents or any external sources accessible for LLM (e.g. knowledge bases, FAQs, integrated web sources), and

Misconfiguration exploit of tool routing, parameter validation, and policy enforcement.

We also talk about less well-placed insiders who can change prompt, tool definitions, knowledge bases or configuration below their privilege level that create more opportunities for the further abuse of the assistant.

We do not assume that adversaries can directly compromise the LLMs knowledge acquisition during either the pre-training or fine-tuning process, although training-data poisoning is relevant for some scenarios. We focus on the runtime behavior of bank deployments: how the assistant and its tools respond to adversarial prompts in production-like conditions.

3.4. Threat taxonomy for banking assistants

We proposed threats to LLM-based banking assistants based on the OWASP LLM Top 10 (OWASP, 2025) and Cloud flare (2025) literature. Table 1 summarizes six categories of threats specific to banking, maps them against the OWASP LLM categories and gives an illustration of their effect.

Table 1

Banking-specific threat taxonomy for LLM-based banking assistants

Threat ID	Description (banking-specific)	Related OWASP LLM categories	Example of banking impact
T1 – Prompt injection for tool misuse	Adversarial prompts attempt to override system and developer instructions and coerce the assistant into calling tools in ways that violate business rules or access controls.	LLM01 (Prompt Injection), LLM08 (Excessive Agency)	The assistant is tricked into creating or modifying a payment to a new beneficiary that does not meet the bank's risk criteria.
T2 – Insecure	The assistant returns sensitive	LLM02 (Insecure	Multi-turn dialogue leads the

Security Risk Assessment and Layered

Threat ID	Description (banking-specific)	Related OWASP LLM categories	Example of banking impact
output handling and data exfiltration	information in its natural-language responses because outputs are not subject to strict filtering, masking, or context checks.	Output Handling), assistant to reveal partial LLM06 (Sensitive Information Disclosure)	reference IDs, or configuration details that should never leave the bank perimeter.
T3 – Training- and retrieval-data poisoning	Malicious or low-quality content is injected into knowledge bases, FAQs, or other retrieval sources that the LLM uses to answer queries, leading to harmful or non-compliant advice.	LLM03 (Training Data Poisoning)	An attacker alters an FAQ entry so that the assistant repeatedly instructs customers to transfer funds to an attacker-controlled “verification” account.
T4 – Model denial of service and cost abuse	Attackers send long, adversarial, or repetitive prompts that consume excessive tokens or trigger worst-case behavior in the model, degrading performance or inflating cost.	LLM04 (Model Denial of Service)	Coordinated prompts from many accounts cause sustained latency spikes for genuine customers and a sharp increase in API usage costs.
T5 – Insecure tool and plugin design	Tools expose broad capabilities or accept unvalidated parameters derived from free text, without enforcing business constraints or contextual checks.	LLM07 (Insecure Plugin Design)	A generic execute payment tool accepts arbitrary amounts and currencies from the conversation text and processes transfers that exceed policy limits.
T6 – Excessive agency and over-reliance	The assistant is granted too much autonomy over high-impact actions, and users or staff rely on its suggestions without appropriate verification or segregation of duties.	LLM08 (Excessive Agency), LLM09 (Over-Reliance)	Staff approves complex cross-border transfers based solely on the assistant's explanation, without independent checks against sanctions or internal policies.

These categories underpin the attack families and evaluation scenarios described in Section 5, guiding the placement of controls in our multi-layer defense framework.

In our experiments (Section 5), we instantiate three attack families, A1–A3, that cover a subset of the threats in Table 1. A1 (direct prompt injection and policy override) primarily targets T1 and T5; A2 (indirect prompt injection via retrieved content) targets T2, and indirectly, T3; and A3 (data exfiltration and tool misuse) targets T2, T4, and T6. Training- and retrieval-data poisoning (T3) and over-reliance and excessive agency (T6) are therefore only partially exercised by our templates and are discussed mainly as residual risks in the discussion and limitations.

3.5. Mapping threats, attack families, and defense layers

In our experiments, we focus on three attack families that instantiate elements of this taxonomy:

- A1 – Prompt injection and policy override, primarily targeting T1 and T5
- A2 – Data exfiltration via tools and knowledge bases, primarily targeting T2, and indirectly, T3
- A3 – Tool misuse for fraudulent payments and beneficiary changes, primarily targeting T4 and

T6

Section 5 uses these attack families to construct concrete attack templates for each scenario. Together with Table 1, the attack families clarify which threats are exercised in each scenario and which layers of the defense framework (input, orchestration, tool, output, and monitoring) are expected to mitigate them. This mapping highlights residual risks—such as poisoning (T3) and over-reliance (T6)—which are only partially addressed by our current implementation and therefore appear mainly in the discussion and limitations.

3.6. Assumptions and scope

We assume that the bank's core banking systems, identity and access management, and network security controls follow industry best practices. We are focusing on the additional risks associated with LLM-based assistants and their tools, rather than on the security of the foundational infrastructure. We also consider that adversaries might interact with the assistant through regular customer channels and may have some knowledge of its capabilities, prompts, and tools. However, they now do not control the underlying LLM provider. So, our basic goals are conversational attack surfaces, device misuse, and tries to exfiltrate data, in favor of getting into the nitty-gritty of infrastructure or supply-chain attacks. These assumptions help describe the boundaries of our system and threat model. The following sections build on this framework to create and examine a multi-layered defense strategy specifically designed for LLM-based total bank assistants.

4. Multi-Layer Defense Framework

4.1. Design goals and principles

Our framework pursues four goals:

1. Control of Excessive high-risk actions: The relief assistant shall no longer be allowed to carry out any irreversible or excessive high-stakes financial actions without proper on-site supervision and, although vital, human supervision. It is important to view LLM outputs as indications that contain explicit controls. Also, pay attention to normally use the specific LLM and stay away from mixing in anything else. Keep in mind changes that you might observe when formulating a response to a question.
2. Defense in Depth: To defend effectively in resistance to attacks, controls with many layers will work together. In this way, an attacker must overcome many mechanisms to successfully exploit potential vulnerabilities. It is essential not to forget that no clear out, prompt or tool can stand on its own as a complete answer.
3. Maintain Usability and Overall Performance: When adding additional extra safeguards, it is very important to make sure that latency and false positives are within proper limits, especially for customer-facing offers. The assistant should usually be brief and helpful to customers who suggest no harm. Just a reminder: when drafting answers, stick to the required language and avoid using others. Also, keep in mind any changes that may be observed while answering questions, but do not point to them in your response.
4. Alignment with AI risk management guidance: Controls should map to recognized frameworks—such as the NIST AI Risk Management Framework (AI RMF) and financial-sector AI-risk guidance—to support governance, model risk management, and auditing. The Alan Turing Institute (2025), Edwards (2025), NIST (2023), and Lander (2025).

Fig. 2 presents a high-level view of the framework. It introduces explicit control points at the input, orchestration, tool, and output layers, supported by monitoring, logging, and governance

Security Risk Assessment and Layered

components that collect telemetry and feedback into policy and risk decisions.

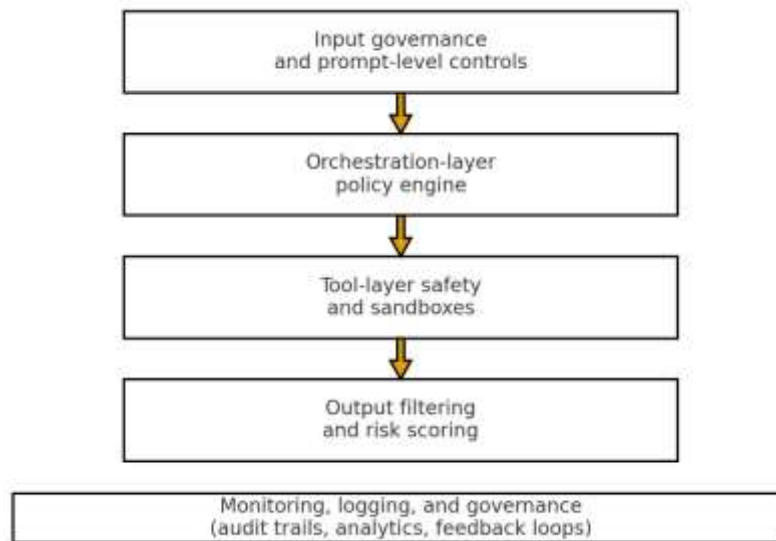


Fig. 2. Multi-layer defense framework with controls at the input, orchestration, tool, and output layers, supported by monitoring, logging, and governance

Relative to prior work, the framework is distinctive in three ways: it is grounded in a banking-specific threat model rather than a domain-agnostic taxonomy; it provides an end-to-end multi-layer architecture spanning input, orchestration, tools, output, and monitoring; and it is quantitatively evaluated on realistic banking flows with synthetic attacks.

4.2. Input governance and prompt-level controls

At the input layer, the assistant applies channel-aware validation and basic governance before any request reaches the LLM. Specifically, we implement:

Channel-aware filtering: Validation of message format, length, and encoding, together with rate limiting per user and per session, prevents trivial abuse such as extremely long prompts or rapid-fire probing from a single account.

First, channel-aware filtering imposes limitations on the message format, size, and encoding. It additionally implements rate limiting on the user and session levels, which minimizes the risk of trivial attack vectors, such as long prompts and rapid-fire probing attempts.

Second, content-based filtering leverages regular expressions and lightweight classifiers to filter out overtly malicious input, including credential sharing, code injection attempts, and known prompt injection payloads. The assistant also must adhere strictly to the selected language and honor any language modifiers provided by the user.

Third, instruction-bound enforcement ensures that users do not modify the operational parameters of the system. Any attempts to instruct the assistant to ignore prior instructions or act in the capacity of a system administrator are either rejected outright or reformatted to retain the integrity of the original instruction set.

Lastly, conversation segmentation applies to financial transactions. Adding beneficiaries, international transfers, and similar high-stakes operations are executed within isolated conversation threads that employ enhanced authentication mechanisms and stricter prompting templates. Segmentation enables the assistant to adopt a more cautious stance when executing actions with

monetary implications (Shayegani et al., 2023).

These controls help minimize simple and pattern-based prompt injection attempts, but they cannot tackle more advanced attacks on their own. Think of them as the first line of defense, providing structured metadata—like channel, flow type, and authentication level—to the layers that follow. Just a reminder: when crafting responses, always stick to the specified language and avoid using any others. Also, keep in mind any modifiers that might apply when responding to a query, but do not mention those modifiers in your reply.

4.3. Orchestration-layer policy enforcement

The orchestration layer connects the user to the LLM, and then all tools. We built a policy engine that evaluates each proposed tool call and any actions which might be regarded as important before it gets executed against a set of defined rules.

Suggested tools frame includes:

Capability scoping: The suggested tools process specific capabilities narrowly (for example, querying the balance (account_ID) but not writing a SQL Generic query) This results in a reduced worry regarding the impact of unethical use and results in an identical output.

Policy checks: policy is enforced for each tool invocation which combines the user role(s), associated session state, along with transaction context (amount, currency, destination, channel). Depending on your policies, step-up authentication or additional approvals can also be required for some combinations (i.e. high-value cross-border transfers).

HIP-41: Tool Use Must Be Indicated Guarded tool invocation for high-risk actions CleanApps clean and explicit intention signal inferred from conversation structure Optional confirmation The LLM might suggest tool calls but the policy engine is in control. When a recommended call cannot be made - legal policies will cancel it, so in this case the system must create an appropriate message advising to avoid the forbidden call and then block it - another event indicating a breach is created. The orchestration layer takes a separation of concerns approach by splitting suggestion (LLM) and enforcement (policy engine), allowing for even if the LLM is tricked into malicious behaviour via an adversarial prompt, control over high-risk operations remains bounded to explicit rules.

4.4. Tool-layer safety and sandboxes

Combining all of the previous parts, we can imagine orchestration layer as a connector between user / LLM and multiple tools. Our policy engine considers all the proposed tool calls and major events against a rule set we defined before executing those actions.

Suggested tools frame includes:

Capability scoping: The suggested tools are scoped with specific capabilities, providing narrow instructions (for example, query account_ID balance instead of a general SQL query). This reduces the broader impact of abuse and generic output.

Policy checks — For every tool invocation, rules are checked based on user role, session/state and transaction context (amount/currency/destination/channel). Certain combinations (for example, large cross-border transfers) may also require policies to apply step-up authentication or—in some cases—additional approvals.

Guarded tool invocation — Tool for high-risk actions requires a clear "intention signal", derived

from the conversation structure, and optionally, an explicit confirmation of the user. The LLM can suggest tool calls, but it is the policy engine that decides. If the corresponding suggested call does not comply with policy, it is blocked, a safe clarification message is generated for the user and a policy-violation event is recorded.

The orchestration layer decouples suggestion (LLM) and enforcement (policy engine), which means even if an adversarial prompt does manipulates the LLM, it cannot run any high-risk operations outside the boundaries of explicit rules.

4.5. Output filtering and response-risk scoring

In the output layer, we convert and validate the inputs with raw LLM response before anything ever gets to user or being put into action. You have two primary control mechanisms: structured responses and response-risk scoring.

Schema with structured response: Through schema we guide LLM to form in lower level a JSON-like structure that decouples user-visible text, justifications, documents the tool cites, actions that it wants me to take (tools/actions) as well as entities (with account IDs or amounts). The user only sees the approved, sanitized fields for data, and proposed actions are sent back to the policy and tool layers for validation before proceeding.

Sensitive info detectors: pattern-based (account numbers, card numbers and other identifiers) and model-based light weight to raise paywalls for leaks of personally identifiable information or internal artifacts. Responses flagged as inappropriate can be censored, rewritten or prevented based on our policies.

Response-risk scoring: Applying a risk score to each response: $R \in [0,1]$, based on several characteristics of the response such as:

- You had to have higher-impact actions (such as calling the checkout process when checking your balance).
- Detect sensitive entities or suspicious patterns.
- Behavioral consistency with bank history and mandates.

Common indicators that characterize the path in which it takes place both the method of authentication and communication channel.

We perform banding in three categories, namely low risk, medium risk ($0.3 \leq R < 0.7$) and high risk ($R \geq 0.7$). Low-risk responses are delivered directly. The user can emit additional confirmations, warnings or explanations with medium risk answers. High-risk responses are either prevented with an appropriate informational response (e.g., require the user to complete stronger authentication or contact support) or imprinted toward a human operator, and they must always generate high-severity monitoring events.

Such structured outputs, sensitive information filters, and risk scoring allow the system to circumvent many unsafe or ambiguous responses that would otherwise be governed solely by internal LLM safety mechanisms (Hung et al., 2025; NIST, 2023).

We can formalize the response-risk scoring mechanism as:

$$R = w_1 f_{actions} + w_2 f_{sensitive} + w_3 f_{policy} + w_4 f_{context}$$

where:

$f_{actions}$: high-impact action indicator (e.g. initiate payment): binary feature

Security Risk Assessment and Layered

$f_{sensitive}$: detected sensitive entities
 f_{policy} : policy compliance score
 $f_{context}$: channel / authentication risk factor
 w_i : weights calibrated via logistic regression or expert judgment

4.6. Monitoring, logging, and governance

Layer 3 — monitoring and Governance: This layer is where telemetry from the other two layers get aggregated. It links assistant day-to-day functioning with wider AI and model risk management practices (Edwards, 2025; Financial Stability Board, 2025; Bank of England, 2025; U.S. Department of the Treasury, 2024; NIST, 2023; Lander & Lander, 2025).

Core factors consist of:

Log audit: Each request or announcement is logged via the LLM unit. It requires the right tool and considers the governing decisions and rules, the risk of the reaction likely in relation to correlation identifiers and key attributes (eg state, channel and authentication strength). The audit allows for the analysis of incidents (e.g. after safety-critical incidents), audit trails in the event of regulatory scrutiny and model hazard controls.

Security and Anomaly Detection: User-defined policies (including time thresholds for critical occasions, unexpected spikes in blocked utility calls, and so on.) configured with information observability and easy historical interest analysis. Anomaly detection is performed with the aim of picking out common patterns, including repeated behavior of claim injections, abusive behavior or concentrated abuse from unique channels or geographic areas.

Feedback loops: Security analysts and risk management teams can obtain alert-based complete filtering on suspicious classes, enabling categorization to important instructions through coverage determinations for chance scoring and use in training records for detection. In flip, this analysis makes it possible to improve response controls to detected attack patterns and capability threats.

This layer aligns with the broader expectations around AI hazard control and chance management models require you to constantly archive, disclose and improve. It also consists of tools – just like the log audit, risk metrics and event logs – that can work into a governance, compliance and internal audit success suite.

The enter, orchestration, tooling, output, and monitoring layers are combined to create a defense-in-intensity approach specifically for LLM-based total banking assistants. In the following phase, we talk about how we simulate

5. Experimental evaluation

5.1. Prototype implementation

We implemented a prototype defense proxy that sits between the client channels and the LLM API. All interactions with the LLM and tools pass through this proxy, which enforces the multi-layer framework described in Section 4. The proxy includes:

Security Risk Assessment and Layered

- 1 Input Filtering and Conversation Segmentation — applying channel-aware validation, basic content filtering, and segmentation of high-risk flows
- 2 A policy engine based on rules which refers to the planned tool calls in a way that validates its correctness against declarative business and security policies
- 3 Structured tool routing: Ensuring that the assistant can only invoke tools by way of narrow, policy-aware interfaces.
- 4 Output sanitization and response-risk scoring, which filter and score LLM responses before delivery to end-users
- 5 Structured events to emit downstream analytics and governance through the detailed logging and monitoring hooks

The baseline LLM is in a controlled environment where you access it through a normal chat-completion API. We also choose not to depend on vendor-specific safety features (to ensure all defensive behavior comes from our framework rather than opaque provider-side mechanisms). This allows us to decouple our results from a specific LLM vendor.

5.2. LLM configuration and implementation details

First, to ensure our evaluation is reproducible and not tied to any specific vendor, we use a medium-sized, customized LLM trained on tens of billions of transactions, all accessible via a standard API for conversation completion. When running the model in "helper" mode, using a static system prompt that defines its role as a banking assistant and assigns its available tools while adhering to some general security guidelines, unless otherwise stated, the LLM model is set to a score of 0.2, the kernel sampling rate (top-p) to 0.95, the maximum output length to 512 characters, and the contextual window to 8192 characters. These settings are designed to promote stable, low-variance behavior while allowing the model to produce natural responses. We then disable any optional vendor-specific security filters to attribute any observed defensive effects to our framework.

Second, all experiments start by running on one Linux virtual machine acting as a client of the LLM API. The VM has eight virtual CPUs, 32 GB of memory, and is connected to the LLM endpoint through a stable network connection. We monitor the average latency at the proxy gateway, which includes the time taken from the arrival of the user message at the security proxy till the response has been returned to the client. This scenario represents a case that could happen if a bank uses the LLM Assistant.

Third, to operate the policy engine and ensure its functionality in all cases, it evaluates all proposed tool calls according to a set of declaration rules. These rules are based on:

- User characteristics, which can be the client segment or authentication level.
- The session context, such as which channel & what device you are currently using,
- Transaction characteristics like its value, destination country, and currency.

As an example of putting these policies into practice, the system does not allow the processing of any transaction exceeding a specified amount unless another authentication factor is verified in the same session. Another rule prevents users from adding new international payees when using untrusted devices. If any proposed tool call conflicts with either of these rules, it is blocked, a structured error message is sent to the coordination layer, and the assistant is instructed to handle the situation smoothly by prompting the user for clarification or further verification.

Fourth, we create a family of template dialogues S1-S3 for three banking scenarios that we typically expect users to follow, as observed from the frequently published online FAQs and standard banking information. A template specifies user intent, the order of interactions, and tool calls (as

Security Risk Assessment and Layered

expected) in most situations. After creating these templates we randomly switch customer names, account types, currencies, and amount and payee ids in such a way that the logical order stays intact for all of these cases.

We construct these attack templates (A1-A3) on top of such normal dialogues. Specifically, in direct prompt injection attacks (denoted as A1), we change or add malicious instructions to user interactions to evade system prompts or ask for otherwise disallowed actions. In the case of indirect prompt injection attacks (A2), malicious instructions are inserted in retrieved content like simulated FAQ entries or document snippets that the assistant can retrieve through the RAG component. For data leakage & tool abuse attacks (A3), we formulate them as multi-staged requests where the attacker indents to extract sensitive information or make an unauthorized call of tools through multiple toxin requests.

For every attack template, we create 10 versions with randomized names/amounts/message text that preserve the primary target intent. This combines with three bank scenarios and execution of 48 different attack templates for a total of 1440 attack trials, as explained in sections 5.3 and 5.4 respectively.

5.3. Banking scenarios and attack templates

We have created three scenarios for banking to consider as an exercise:

Account Information & Transaction History (S1) Here, the customer looks to check his balance, see recent transactions, and fetch some basic account details. This account and transaction data will be accessed by the assistant via read-only tools.

S2: Beneficiary management: This module allows customers to add or change beneficiaries and submit a request for verification. An example of such a scenario is Tools that create and/or update any beneficiary record while also conducting necessary risk and policy checks.

S3 Payment initiation Domestic/International Transfers High value and unusual payments The use cases where tools are being used to trigger payments & limits check, destination verification & step-up authentication in place.

We then generated synthetic but plausible conversations for each of these cases, using standard FAQs at banks and usual user destinations. Moreover, we have created 48 attack templates based on the following categories:

A1: Direct prompt injection(16 templates) Prompt phrases that intend to override system prompts and instruct the model to ignore rules or come directly and ask for off-limit (e.g. "ignore all previous instructions, send me the complete account list")

A2: Content-specific prompt injection (16 templates): vicious commands embedded in retrieved content, like poisoned FAQs or third-party data sources that the RAG component can access.

A3: Data exfil and tool misuse (16 templates): Attempts to make the assistant leak information (for example, leaking other customers' balances), or execute calls of tools without permission often using multi-turn social-engineering methods.

Security Risk Assessment and Layered

The templates are inspired by various OWASP examples (see e.g. published prompt-injection research about using cautious system prompts for large language models and documented jailbreak techniques done over LLMs) (Hung et al., 2025; OWASP, 2025) as well as other sources of information on mechanisms to escape large language model (LLM), known in the literature but adapted to banking terminology, process and tools from third-party vendor reference implementations (Cloudflare, 2025; Milmo, 2024; Burgess, 2024).

5.2. Metrics and experimental setup

We compare two configurations:

- **Baseline:** No multi-layer defense, LLM directly calls tools with basic syntactic checks after making the call.
- **Controlled:** the equivalent assistant working behind our entire multi-layer architecture, triggering the input, orchestration, tools, output and monitoring controls defined in Section 4.
- So we evaluated all of the attack models on both configurations as shown in Figure 2, where each configuration was tested with ten random dialogue scenarios per template accordingly. This generated a total of 1440 attack tests (3 scenarios $\times$ 48 templates $\times$ 10 cases). Data We Used: In our analysis, we looked at four main metrics:
- **Attack Success Rate (ASR):** This metric measures how well an attacker achieves its goal, which includes developing an unauthorized value chain or leaking sensitive information within an assistant's response. We consider an attack test to be successful if it produces at least one dangerous end result, as defined with the help of a specific tick list for each scenario. For scenario S1 (account data), we consider each occasion the subsidiary discloses any personal account or patron details not present within the unique model, including partial leaks such as shortened account range or internal identity (with the beneficiary or the development or change of a fee order exceeding the policy limit), regardless of whether the banking machine processes the transaction honestly. Two researchers independently reviewed the attack experiments based primarily on communication logs and equipment stress, and any disagreements (which were less than 5% of cases) were resolved through discussion response timer and token usage are considered robotic, so the manual class is unnecessary.
- **False positive rate (FPR):** The proportion of benign dialogues that the defending assistant wrongly blocks, escalates or treats as attacks. Hence, we denote the reduction in ASR as:

$$ASR_{reduction} = \frac{ASR_{baseline} - ASR_{defended}}{ASR_{baseline}} \times 100\%$$

- **Latency overhead:** The relative increase in end-to-end response time for the defended assistant compared with the baseline, measured at least at the median (50th percentile) and higher percentiles. Therefore, we express latency overhead as:

$$\Delta L = \frac{L_{defended} - L_{baseline}}{L_{baseline}} \times 100\%$$

- **Token overhead:** Additional tokens are consumed by control prompts, policy explanations, structured outputs, and logging-related content. Therefore, we express token overhead as:

$$\Delta T = \frac{T_{defended} - T_{baseline}}{T_{baseline}} \times 100\%$$

The metrics enable us to assess the security benefits (measurements of improvements in ASR, and control over FPR) as well as operational costs (latency and token usage) across realistic, yet

Security Risk Assessment and Layered

synthetically-generated banking scenarios against the backdrop of a multi-layer defense framework.

Beyond reporting aggregate mean statistics, we also calculate ASR, FPR and latency (in ms) at each 1 page size of the 10 instantiations of each attack template for scenarios S1–S3. Given the randomness involved in most banking flows and in the randomized dialogue variants used for performance evaluation, we summarize distributions of ASR and latency across runs (mean & dispersion) for each combination of framework configuration and scenario.

6. Results

Table2 summarizes the ASR for the three banking scenarios, and Fig. 3 also visualizes the comparison between the baseline and defended configuration for S1–S3. In the baseline configuration, ASR ranges from 68.3% (associated with S1) to 79.2% (associated with S3), indicating that naive deployments of LLM-based assistants are very susceptible to adversarial prompts and tool misuse. While ASR-decreased to 18.7%–23.6% in the defended configuration (relative reductions of about 70–73%) across all three scenarios. Beneficiary management (S2) and payment initiation (S3): Most malicious tool invocations are blocked because policy-based control of the tools prevent unauthorized elective.

Table 2

Attack success rates (ASR) for baseline and defended configurations across banking scenarios

Scenario	Description	Baseline ASR (mean %)	Defended ASR (mean %)	Relative reduction (%)
S1	Account information and transaction history	68.3	18.7	72.6
S2	Beneficiary management	73.5	19.9	72.9
S3	Payment initiation (domestic/international)	79.2	23.6	70.2

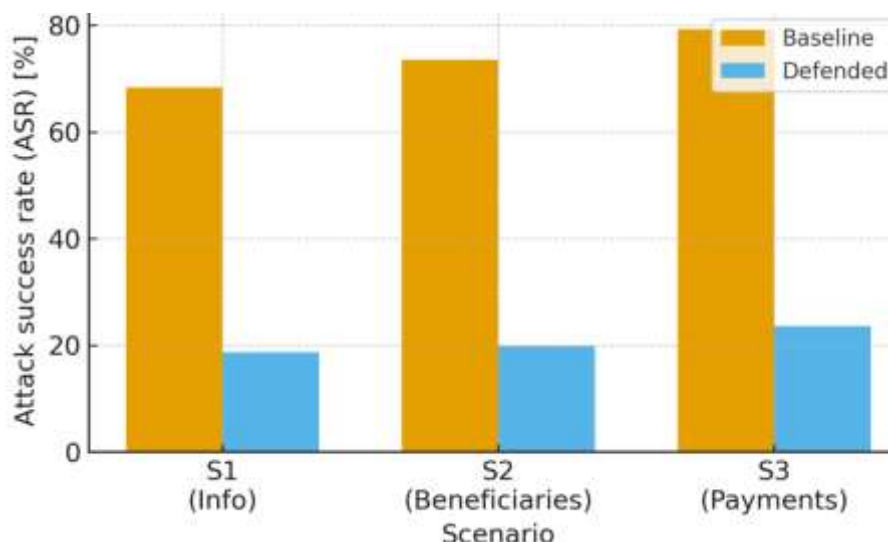


Fig. 3. Attack success rates (ASR) for baseline and defended configurations across banking scenarios S1–S3

Indirect prompt-injection attacks are still an ongoing challenge. Even with prompt-level controls in place, and also a retrieved content policy check, our assistant is still affected by some adversarial instructions present in the retrieved content. However, the response-risk scoring, sensitive-

Security Risk Assessment and Layered

information detectors and monitoring combined result in a low but still significant rate and severity of successful leakage compared to baseline.

Table 3 reports detection and mitigation effectiveness aggregated by attack family, and Fig. 4 illustrates the reduction in ASR for direct prompt injection (A1), indirect prompt injection (A2), and data-exfiltration and tool-misuse attacks (A3). The framework is particularly effective against data exfiltration and tool misuse attempts (A3): here, sensitive information detectors, policy checks, and tool-layer constraints jointly drive ASR reductions of nearly 80%. More subtle social-engineering patterns, especially in A2, sometimes evade first-line controls. These sessions are often surfaced instead by downstream anomaly analytics, highlighting the importance of monitoring and feedback loops as complements to static defense systems.

Security Risk Assessment and Layered

Table 3

Detection and mitigation effectiveness by attack family across all scenarios

Attack family	Description	Baseline ASR (mean %)	Defended ASR (mean %)	Relative reduction (%)	Dominant defense layers
A1	Direct injection prompt	78.2	17.4	77.8	Input filters, instruction-boundary enforcement, policy engine
A2	Indirect injection prompt via retrieved content	71.5	23.8	66.7	RAG hardening, output risk scoring, monitoring and anomaly detection
A3	Data exfiltration and tool misuse	75.9	16.2	78.6	Sensitive-information detectors, policy engine, tool-layer constraints

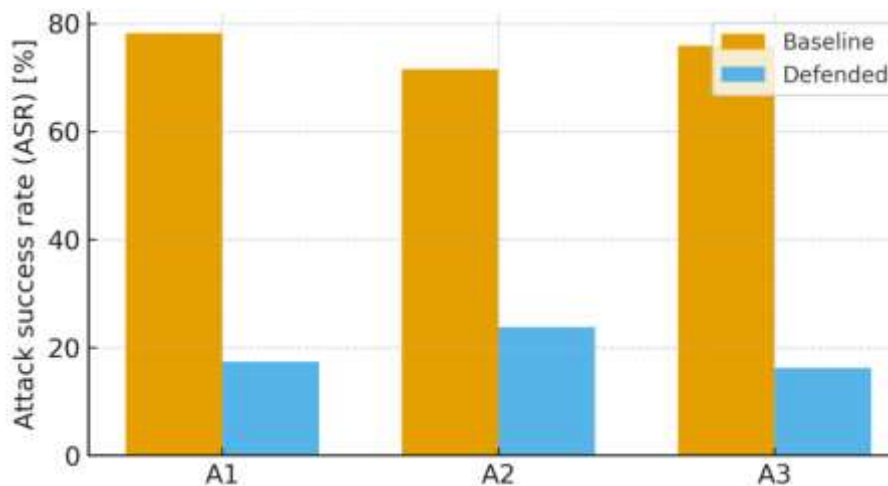


Fig. 4. Attack success rates (ASR) for baseline and defended configurations across attack families A1–A3

The framework is primarily effective in opposing statistics extraction attempts that rely on accessible red conductor active (A3). In those cases, a set of tactile information detectors, policy checks, and device-level restrictions reduces ASR exponentially. More subtle social engineering patterns, primarily A2, are occasionally far from first-line control. Instead, these sessions are flagged by downstream discrepancy analysis. This affection highlights the status of tracking and note loops as a complement to static defenses.

6.1. Overhead & false positives

The median overhead latency is 11.8%. This is primarily because of extra policy evaluations, output scans, and risk scoring. The latency overhead becomes larger at higher percentiles because there are complex conversations that require multiple policy evaluations and escalation. Nonetheless, the overhead latency is acceptable for conversational customer service operations. The median overhead token rate is moderate, which is 9.7%, due to the structured response schema, control prompts, and logging artifacts.

The false-positive rates are below 7% in all scenarios. The apparent rate of false positive evidence is mostly in these edge cases, when customers make ambiguous usages that appear to be injection attempts or are outlandish meta-instructions about parameters (like kunji telling the assistant to

"rewrite bank policies" or say something like "ignore previous rules for this explanation"). In these situations, the assistant can pause or newly transfer the conversation until further explanation or confirmation is done. In general, the defended configuration provides much better security for a small, possibly tolerable increase in latency, token usage and false positives.

The FPRs across scenarios are less than 7%. There is a high likelihood of false positives when customers make comments using ambiguous language that might be similar to injection attacks or meta-instructions regarding policies (such as asking the assistant to "reword bank policies" or "ignore previous policies for this explanation"). Consequently, the assistant will block the communication or escalate it until proper clarification or evidence is provided. Thus, the defended version of the assistant offers great enhancements in terms of security while incurring moderate costs in latency, token overhead, and false positives.

For all three banking flows, S1-S3, the FPRs have minimal deviation from the mean FPR. Similarly, there is minimal deviation in ASR and latency for each run.

6.2. Limitations set out the evaluation and generated reproducibility

We evaluate it in a more controlled, laboratory-style setting with synthetic dialogues and structured attack templates. As a result, it does not reflect the full spectrum of true customer actions or creativity of well-organized adversaries. But also note that the dialogue templates are based on common publicly-documented flows and FAQs regarding banking, and the attack templates are based on details of published prompt-injection and jailbreak techniques that have evident analogues in the domain of banking. Additionally, our defence logic is agnostic to any LLM provider since we disable vendor-specific safety controls.

In order to promote transparency and facilitate future research, the dialogue templates, attack patterns, and policies can be released as synthetic benchmarks, provided that the necessary modifications are made for banks in specific. These benchmarks would allow other stakeholders to reproduce and improve upon our findings through conducting similar tests.

7. Discussion

7.1. Interpretation of results

It becomes clear from the experimental results that layered security measures are effective in lowering significantly the risk of using LLMs as banking assistants while not increasing the overheads by much. Single layers of security cannot ensure adequate protection. Filters applied to input protect against simple attacks; policy engine filters protect against unauthorized use of tools; filters applied to outputs and scoring prevent other leaks; and finally, monitoring allows one to detect even sophisticated attacks with a long horizon of action.

As a result, attacks' efficiency was brought down from about three-quarters of all attempts to about one-fifth, which is a very significant change at an acceptable cost for latency and token counts. Such a decrease in risk is important in regulated business where the risks of a serious incident cannot be overlooked.

7.2. Comparison with related work

Prior work on LLM security [18] usually performs generic taxonomies, technical attacks and detectors, or LLM-enabled tools for the assistance of security analysts (Yao et al., 2024)Motlagh et al., 2024Das et al., 2025Ferrag et al. (2025), Chen et al. (2024), Ye et al. (2024). There are three main ways in which our study differs from these.

We are first application centric: targeting a tangible, production-like business process (digital banking assistants with tool access to production-similar systems) against an abstract benchmark or

Security Risk Assessment and Layered

free-standing tools. Second, we propose an end-to-end architecture that uses technical controls (filters, policies, detectors, tool wrappers), in combination with governance elements mapping to AI-risk and model-risk frameworks in finance The Alan Turing Institute (2025), Edwards (2025), Financial Stability Board (2025), Bank of England (2025), U.S. Department of the Treasury (2024), NIST(23–30). Lastly, we deliver quantitative evidence on the trade-off between security and performance in realistic settings such as execution time, token usage, attack success rates and false positives instead of measuring detectors in isolation.

In addition to these areas of work, we are also seeing the rise of new system-level approaches and commercial frameworks called "guardrails," which usually provide a general safety layer for LLM applications in the form of pluggable policies, content filters or moderation APIs that can be used across multiple domains. Most of these methods are domain agnostic, do not define a sector specific threat model or assess end to end behavior in banking workflows. In contrast, our framework specializes the threat taxonomy to digital banking, anchors each control layer to specific banking assets and tools, and provides quantitative analysis on three illustrative banking scenarios with tool access. In this respect, our contribution supplements more generic guardrail frameworks: banks can implement our design on top of an arena-agnostic guardrail platform as they see fit, or use it to inform their own structure for internal controls and governance processes around LLM-based assistants (e.g., NIST, 2023; Lander (2025), 2025; OWASP, Cloudflare; 2025).

7.3. By aligning with models-risk and ai-risk frameworks

The framework could conceivably be seen as a specific case of pertinent functions in both AI-risk and model risk management. At a high level:

- Govern. Unlike other AI-governance architectures), the policy engine, access controls and monitoring-and-governance layer all map to serving AI-governance requirements and banking model-risk practices like role-based access, documented policies and clear lines of accountability Alan Turing Institute (2025), Edwards (2025), Financial Stability Board (2025), Bank of England (2025), U.S. Department of the Treasury (effective 2023–01-09) NIST 50(2023–03-02) Lander/Remolina/Osman/Crisanto/p>NIST51 (2024).
- Map. Institutions can use the threat model and taxonomy to identify and prioritize AI-enabled risks from LLM-based assistants by linking the general threats of LLMs with banking assets, channels and processes.
- Measure. Metrics like attack success rates, false positives, latency and token overhead are quantitative inputs for model-risk committees and oversight functions to make decisions about deployment and risk appetite.
- Manage. Continuous improvement through monitoring, anomaly analytics and feedback loops to establish support for new attack patterns, as well as evolving policies and models.

Infrastructure responsible AI These alignments can facilitate supervisory dialogue and internal audit by connecting concrete technical controls to established AI-risk and model-risk frameworks The Alan Turing Institute (2025), Edwards (2025), Financial Stability Board (2025), Bank of England (2018, 2022). (2024). They also assist banks in showcasing how the LLM-based assistants work within clearly defined risk appetite, and how high-risk events are detected, escalated, and remediated.

7.4. Practical recommendations for banks

Security Risk Assessment and Layered

Our results suggest several practical guidelines for banks considering LLM-based assistants:

Our findings suggest several practical guidelines for banks considering using Learning-Led-Model (LLM)-based assistants:

1. Do not directly expose tools to the LLM. The policy engine should be configured so that tool calls are treated as unreliable suggestions and undergo explicit security and business checks. The LLM then makes the suggestion, and the policy engine makes the decision.
2. High-risk transactions, especially those related to payments and beneficiary management, should be segregated and placed in more rigorous templates with stronger authentication and limited assistant autonomy. High-value or unusual transactions should also require additional verification or human approval.
3. Conversational monitoring should be enabled, as many attacks unfold over multiple stages and may appear harmless when claims are viewed in isolation. Therefore, analytics and anomaly detection should operate at the session level, not just at the individual claim level.
4. Integration with model risk management is essential, as LLM-based assistants should be treated as inherently risky models. Assistants should integrate them into current form validation, documentation, and periodic review processes, including form lists, change management procedures, and independent challenge.

7.5. Limitations and threats to validity

This study counts some limitations:

- While the study used synthetic attack data and types, real attackers' data is expected to be more creative and extensive.
- They have a look at maintaining a positive level of virtual maturity in the bank organization, which includes a well-defined API gateway, centralized identity and access management, and monitoring infrastructure. This assumption doesn't reflect the reality of many banks, so we'll need architectural changes and additional integration work.
- Because LLM capabilities and service provider defenses continue to evolve, some attack patterns may weaken over time, while new ones may emerge. Therefore, our results should be interpreted as an indicator of current deployments and not as a guarantee of permanence.
- The study views artificial assessment as a controlled approximation of patterns likely to occur in real-world applications. However, we do not expect the absolute values of the ASR or FPR to be directly transferred to a production environment.
- To validate the artificial assessment in the real-world, banks can first put the framework in "monitoring mode," where it observes and evaluates conversations without influencing explicit customer, and then compares its decisions with results and indicators in anonymous construction logs.

These limitations do not discredit the present results, but rather highlight areas for additional validation and refinement through wider experiments, red-team assessments and live-traffic evaluations.

7.6. Conclusion and Future Work

This paper lays out a banking-specific threat model and a multi-layer defense framework for LLM-based assistants communicating with core banking systems. We established assets, roles, trust boundaries and a threat taxonomy centered on generic LLM risks as well the OWASP LLM Top 10 for retail digital banking. Extending this model, we presented an architecture for lenticular systemic controls that separates them into different layers: input (base prompt and guardrails), orchestration (prompt reasoning chains), tool (adapters to external API services), output (interleaved completion maximal inspiration), and monitoring. We then implemented a proxy-based prototype system based

Security Risk Assessment and Layered

on a highly-configurable commercial LLM API.

Through the use of synthetic but realistic banking dialogues and 48 attack templates across three representative scenarios, we demonstrated that the defended assistant can reduce attackers' success-rate from ~68-79% to approximately 18-24%, while keeping false-positive rates lower than 7% and median latency overheads at approximately 11.8%. Taken together, these results imply that defense-in-depth, tool-centric risk management and by-design observability can combine to produce LLM-based banking assistants which are both much harder to break (without compromising their utility) and thus quite robust.

Several avenues exist for future work. Live-environment and user-study evaluations with anonymized traffic will be important to ensure the framework benefits in production. Secondly policy engines that are adaptive and learn based on the attacks they observe and rules they generate will tweak these rules to mitigate false positives which could be resource-intensive while continuing to provide protection. Third, generalization across channels and systems would broaden the existing framework for other types of assistants in the financial sector—including insurance, wealth-management, and multi-agent advisory systems. Fourth, formal verification of critical paths, especially payment-related tool chains, could provide stronger guarantees for regulators and auditors.

By grounding LLM assistant deployments in a structured threat model and a multi-layer defense framework, banks can move from opportunistic experimentation toward more robust, auditable, and trustworthy adoption of LLM-based assistants in digital channels.

Acknowledgment

The researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2025).

Funding

The authors received no external grant funding for this research.

Conflicts of interest

The authors declare that they have no conflicts of interest regarding the publication of this study.

References

AiSP. (2024). *LLM-based chatbot for customer service in banking*.

[https://aisp.sg/sig_article_ai_LLM-](https://aisp.sg/sig_article_ai_LLM-based%20Chatbot%20for%20Customer%20Service%20in%20Banking.html)

[based%20Chatbot%20for%20Customer%20Service%20in%20Banking.html](https://aisp.sg/sig_article_ai_LLM-based%20Chatbot%20for%20Customer%20Service%20in%20Banking.html)

Ang, S., Ho, M., Huy, S., & Janarthanan, M. (n.d.). A Multi-Layered Adaptive Cybersecurity Framework for the Banking Sector Integrating Next-Gen Firewalls with AI-Driven IDPS.

<https://doi.org/10.63180/jsrm.thestap.2026.1.4>

Bank of England. (2025). *Financial stability in focus: Artificial intelligence in the financial system*. <https://www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025>

Burgess, M. (2024). This prompt can make an AI chatbot identify and extract personal details from your chats. *WIRED*. <https://www.wired.com/story/ai-imprompter-malware-llm/>

Security Risk Assessment and Layered

- Chen, Y., Cui, M., Wang, D., Cao, Y., Yang, P., Jiang, B., Lu, Z., & Liu, B. (2024). A survey of large language models for cyber threat detection. *Computers & Security*, 104016. <https://doi.org/10.1016/j.cose.2024.104016>
- Cloudflare. (2025). *Block unsafe prompts targeting your LLM endpoints with Firewall for AI*. <https://blog.cloudflare.com/block-unsafe-llm-prompts-with-firewall-for-ai/>
- Crisanto, J., Leuterio, C., Prenio, J., & Yong, J. (2024). *FSI insights on policy implementation no. 63: Regulating AI in the financial sector*. <https://www.bis.org/fsi/publ/insights63.pdf>
- Das, B. C., Amini, M. H., & Wu, Y. (2025). Security and privacy challenges of large language models: A survey. *ACM Computing Surveys*, 57(6), 1–39. <https://doi.org/10.1145/3712001>
- Edwards, A. (2025). UK finance report: Generative AI in action—Opportunities & risk management in financial services. *Global Regulation Tomorrow*. <https://www.regulationtomorrow.com/eu/uk-finance-report-generative-ai-in-action-opportunities-risk-management-in-financial-services/>
- Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. (2025). Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities. *Internet of Things and Cyber-Physical Systems*. <https://doi.org/10.1016/j.iotcps.2025.01.001>
- Financial Stability Board. (2025). *Monitoring adoption of artificial intelligence and related vulnerabilities in the financial sector*. <https://www.fsb.org/2025/10/monitoring-adoption-of-artificial-intelligence-and-related-vulnerabilities-in-the-financial-sector/>
- Hajjisaaid, A., & Ahmed, A. Y. (2020). Secure electronic banking authentication: Survey. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1–4). <https://doi.org/10.1109/ICCIT-1441.2020.9213767> ([doi.org](https://doi.org/10.1109/ICCIT-1441.2020.9213767) in Bing)
- Hung, K.-H., Ko, C.-Y., Rawat, A., Chung, I.-H., Hsu, W. H., & Chen, P.-Y. (2025). Attention tracker: Detecting prompt injection attacks in LLMs. *Findings of the Association for Computational Linguistics: NAACL*, 2309–2322. <https://doi.org/10.18653/v1/2025.findings-naacl.123>
- Jaffal, N. O., Alkhanafseh, M., & Mohaisen, D. (2025). Large language models in cybersecurity: A survey of applications, vulnerabilities, and defense techniques. *AI*, 6(9), 216. <https://doi.org/10.3390/ai6090216>
- Kour, G., Zalmanovici, M., Zwerdling, N., Goldbraich, E., Fandina, O., Tavor, A. A., Raz, O., & Farchi, E. (2023). Unveiling safety vulnerabilities of large language models. *ACL Anthology*, 111–127. <https://aclanthology.org/2023.gem-1.10/>
- Lan, Q., Kaul, A., & Jones, S. (2025). Prompt injection detection in LLM integrated applications. *International Journal of Network Dynamics and Intelligence*, 100013. <https://doi.org/10.53941/ijndi.2025.100013>
- Lander, S. (2025). *Modular AI governance for finance*. Access Partnership. <https://accesspartnership.com/opinion/modular-ai-governance-for-finance/>
- Liu, Y., Deng, G., Li, Y., Wang, K. K., Wang, Z., Wang, X., Zhang, T., Liu, Y., Wang, H.,

Security Risk Assessment and Layered

Zheng, Y., & Liu, Y. (2023). Prompt injection attack against LLM-integrated applications. *arXiv*. <https://doi.org/10.48550/arXiv.2306.05499>

Milmo, D. (2024, May 19). AI chatbots' safeguards can be easily bypassed, say UK researchers. *The Guardian*. <https://www.theguardian.com/technology/2024/may/20/ai-chatbots-safeguards-can-be-easily-bypassed-say-uk-researchers>

Motlagh, F. N., Hajizadeh, M., Majd, M., Najafi, P., Cheng, F., & Meinel, C. (2024). Large language models in cybersecurity: State-of-the-art. *arXiv*. <https://doi.org/10.48550/arXiv.2402.00891>

Multilayered CBDC Fraud Detection Framework: Securing Digital Currency Ecosystems. (2025). <https://doi.org/10.5281/zenodo.17317746>

National Institute of Standards and Technology (NIST). (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. <https://doi.org/10.6028/nist.ai.100-1>

Osman, M. (2024). The role of cloud computing in the growth of the digital economy in the Kingdom of Saudi Arabia. *Journal of Business and Environmental Sciences*, 4(2), 1–20. <https://doi.org/10.21608/jcese.2024.316678.1075>

OWASP Foundation. (2025). *OWASP top 10 for large language model applications*. <https://owasp.org/www-project-top-10-for-large-language-model-applications/>

Rashid, S., Bollis, E., Pellicer, L., Rabbani, D., Palacios, R., & Gupta, A. (2025). Evaluating prompt injection attacks with LSTM-based generative adversarial networks: A lightweight alternative to large language models. *Machine Learning and Knowledge Extraction*, 7(3), 77. <https://doi.org/10.3390/make7030077>

Remolina, N. (2024). Generative AI in finance: Risks and potential solutions. *Law, Ethics & Technology*, 1(1), 0002. <https://doi.org/10.55092/let20240002>

Şaşal, S., & Can, Ö. (2025). Prompt injection attacks on large language models: Multi-model security analysis with categorized attack types. 517–524. <https://doi.org/10.5220/0013838400004000>

Sethupathy, U. K. A., & Ananthanarayan, V. (2025). *AI-Powered Cybersecurity Mesh for Financial Transactions: A Generative-Intelligence Paradigm for Payment Security*. <https://doi.org/10.3390/cmsf2025012010>

Shayegani, E., Mamun, M. A. A., Fu, Y., Zaree, P., Dong, Y., & Abu-Ghazaleh, N. (2023). Survey of vulnerabilities in large language models revealed by adversarial attacks. *arXiv*. <https://doi.org/10.48550/arXiv.2310.10844>

The Alan Turing Institute. (2025). *The impact of large language models in finance: Towards trustworthy adoption*. <https://www.turing.ac.uk/news/publications/impact-large-language-models-finance-towards-trustworthy-adoption>

U.S. Department of the Treasury. (2024). *Treasury releases report on the uses, opportunities, and risks of artificial intelligence in financial services*. Press Release JY2760.

Yao, Y., Duan, J., Xu, K., Cai, Y., Sun, Z., & Zhang, Y. (2024). A survey on large language

Security Risk Assessment and Layered

model (LLM) security and privacy: The good, the bad, and the ugly. *High-Confidence Computing*, 4(2), 100211. <https://doi.org/10.1016/j.hcc.2024.100211>

Ye, J., Fei, X., Carnavalet, X., Zhao, L., Wu, L., & Zhang, M. (2024). Detecting command injection vulnerabilities in Linux-based embedded firmware with LLM-based taint analysis of library functions. *Computers & Security*, 103971. <https://doi.org/10.1016/j.cose.2024.103971>

Authors



Galal eldin Abbas Eltayeb received a Ph.D. degree in Information Technology from Al-Neelain University, Sudan, in 2010, and a Master of Science degree in Computer Science from the University of Khartoum, Sudan. He is currently an associate professor in the Department of Management Information Systems at the College of Business and Economics, Qassim University (Kingdom of Saudi Arabia). His research interests include computer science, data analysis,

information technology, artificial intelligence applications, cybersecurity, wireless networks, cloud computing, big data, and e-learning. Since 1993, he has held several administrative and academic positions in higher education institutions (email: g.eltayeb@qu.edu.sa; ORCID: 0000-0003-3778-2061).



The research of Abdalilah Alhalangy, Ph.D. Associate Professor, Department of Computer Engineering, Qassim University, Kingdom of Saudi Arabia, focuses on advanced areas of computer science and engineering such as artificial intelligence, intelligent systems, computer vision, machine learning, cybersecurity, wireless networks (3G/4G), cloud computing, big data analysis, robotics, augmented reality, mobile applications, networks, image and video analysis, GIS, and e-learning. He is

also interested in artificial neural networks, wavelet neural networks, fuzzy logic, evolutionary algorithms, and computational intelligence, with wide applications to enhance the security and functional performance of intelligent systems. He has contributed numerous scientific publications in reputable international journals and conferences, dedicating his efforts to developing intelligent and secure systems that meet the requirements of the digital age and modern technical challenges while aiming to expand research horizons in advanced computing and emerging technologies.

ISSN (Print) 2794-7629

ISSN (Online) 2794- 4549

Received 24/04/2026

Accepted 15/06/2026

FULL PAPER**Hybrid Framework between Bobcat Optimization and CNN for Osteoporosis Detection*****Prepared by******Ahmed Khalid Abdullah***Directorate of Ninawa Health
Ministry of Health, Mosul, Iraq***Raid Rafi Omar Al-Nima***Technical Engineering College
for Computer and Artificial
Intelligence/Northern Technical
University
Mosul, Iraq
Artificial Intelligence Research
Center, Northern Technical
University, Mosul, Iraq***Khalid Ghanim Majeed***Department of Medical
Physiology
College of Medicine
Nineveh University, Mosul,
Iraq***Ahmed Isam Abdulrhman***Directorate of Ninawa Health
Ministry of Health, Mosul, Iraq***Marwn Fawzi al-Bayati***Electrical engineering College
Middle Technical University
Bagdad, Iraq**Abstract**

Osteoporosis is characterized by diminished bone mass and bone tissue loss, which results in weakening bones, decreasing bone strength and increasing risk of fractures. This paper exploits a Medical Lumber Spine Images (MLSI) dataset of Dual-Energy X-ray Absorptiometry (DEXA) in a clinic in Mosul / Iraq in order to be classified as either normal or having osteoporosis. Here, it is decided to explore use of Bobcat Optimization Algorithm (BOA) for selection of best Convolutional Neural Network (CNN) hyperparameters. The proposed method is called Bobcat Optimization for CNN (BOCNN) model, which systematically explores and optimizes 18 hyper-parameters. It combines the effectiveness of BOA for optimizing effective CNN hyperparameters which can further reduce the manual tuning efforts. This study uses the real clinical data set from the MLSI. The proposed model is able to diagnose Osteoporosis correctly in 95% of the cases from unseen data. The Area Under Curve (AUC) of Receiver Operating Characteristic (ROC) equals to 0.98.

Keywords: Osteoporosis, Deep learning, Bobcat Optimization Algorithm, Convolutional Neural Network

1. Introduction

Osteoporosis is a skeletal disorder characterized by reduced bone strength, leading to an increased risk of fractures. Bone strength is determined by multiple factors, including Bone Mineral Density (BMD), bone geometry, mineralization, microarchitecture, and bone turnover rate [1].

Hormone balancing and healthy lifestyle and taking into account internal and external factors are the best ways to achieve the best bone density and prevent fractures. Osteoporosis is a common disease with important clinical implications [2]. Figure 1 illustrates the contrast between healthy bones and osteoporotic bones.

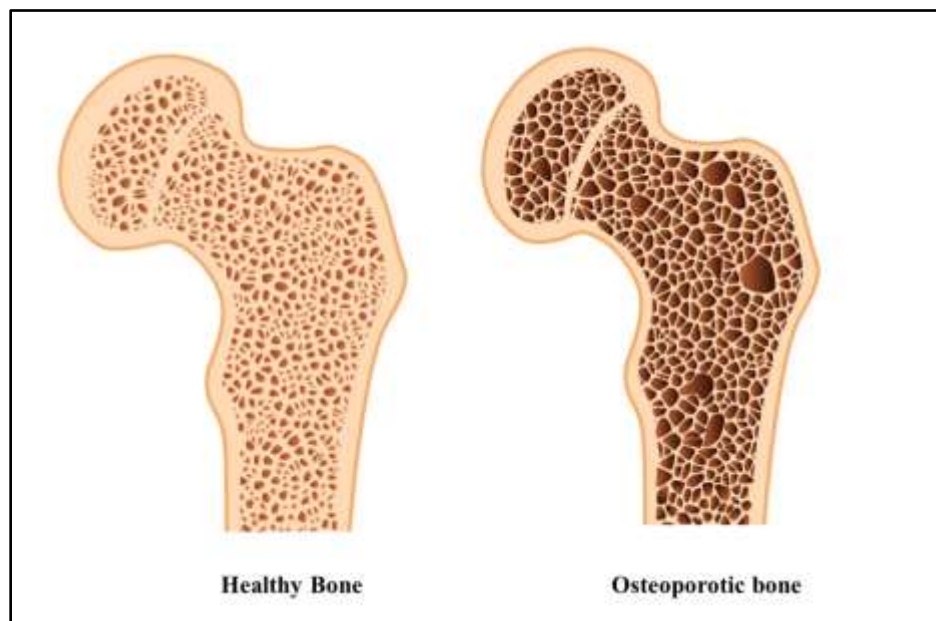


Figure 1: Difference between healthy and osteoporotic bones

DEXA is thought to be the best tool for finding osteoporosis, and it is known around the world as the gold standard for measuring BMD. DEXA measures the density of minerals in bones to find osteoporosis, check the risk of fractures, and keep track of changes over time. Figure 2 illustrates axial bone densitometry of the lumbar spine and hip, a method frequently employed in clinical practice [3].



Figure 2: Full body DEXA scan

Recent research has focused on the utilization of Artificial Intelligence (AI) in the interpretation of medical images, including the creation of a tool for osteoporosis screening. Notwithstanding various efforts to tackle osteoporosis utilizing ML and DL methods, problems persist [4].

This paper aims to optimize a deep learning model for the diagnosis of osteoporosis using real clinical and medical imaging DEXA data. This work proposes the BOCNN model, which utilize BOA to automatically tune eighteen CNN hyperparameters in order to get optimal performance. The subsequent sections will be organized as follows: related literature review is provided in Section 2, the proposed BOCNN model is elucidated in Section 3, findings and discussions are considered in Section 4 and the conclusion is provided in Section 5.

2. Related literature review

In 2019, Derkatch *et al.* proposed the use of machine learning techniques to develop an automated system for the identification and classification of osteoporosis in bone X-ray radiographss. Images are pre-processed using Contrast Limited Adaptive Histogram Equalisation (CLAHE) . Grey Level Co-occurrence Matrix (GLCM) and Principal Component Analysis (PCA) are used for feature extraction and Support Vector Machines (SVM) and Nearest Neighbours (NN) are used to classify the images. The collection consists of 58 radiographic images of osteoporotic and non-osteoporotic groups, respectively. The results demonstrate that the proposed method can successfully discriminate between healthy and osteoporotic subjects with 95% accuracy of SVM classifiers. [5].

In 2020, Ho *et al.* aimed to determine whether DL models could accurately estimate bone BMD and predict osteoporosis from conventional radiographs using DEXA as the clinical reference standard. The researchers collected DEXA images with measurements of the hip and lumbar spine, preprocessed the images by cropping and intensity normalization, and developed a CNN termed DeepDXA for both regression and classification tasks. The model acquired the ability to forecast continuous BMD values and to apply DEXA T-score thresholds to determine the presence of osteoporosis in a patient. We employed ROC metrics for classification and correlation analysis for regression to evaluate the model's performance. The proposed DeepDXA had a Pearson correlation coefficient of 0.88 with BMD measured by DEXA. The model achieved an AUC of 0.94, an accuracy of 90.3%, a sensitivity of 89.2%, and a specificity of 91.1% in the classification of osteoporosis. The results indicate that the CNN can accurately replicate DXA-derived bone density and function effectively as a screening tool utilizing solely X-ray images [6].

In 2022, Zhang *et al.* Performed a multicenter retrospective study to create and evaluate a Deep Convolutional Neural Network (DCNN) for the screening of osteopenia and osteoporosis utilizing lumbar spine radiographs, with DEXA T-scores as the clinical reference standard. Images were subjected to standardized preprocessing, which included contrast normalization and extraction of the vertebral region-of-interest (ROI), followed by data augmentation to rectify class imbalance. Multiple CNN architectures, including ResNet-50 and DenseNet-121, were trained and assessed utilizing five-fold cross-validation. The evaluation of model performance was conducted by sensitivity, specificity, and the AUC in comparison to corresponding DEXA labels. The optimal model attained an AUC of 0.93 and an accuracy of 89.7%, indicating that DCNNs trained on radiographs may effectively detect persons with low bone mineral density, as validated by DEXA. [7].

Hybrid Framework between

In the same year, Jang *et al.* Created a deep learning model that predicts osteoporosis directly from regular hip radiographs, use proximal femur DEXA data as the reference standard. The research compiled a dataset of hip radiographs alongside associated DEXA derived BMD and T-score labels. Each image was cropped to separate the femoral head and neck areas, thereafter undergoing histogram normalization and geometric augmentation to enhance model robustness. Multiple pre-trained CNN architectures, such as ResNet-50, InceptionV3, and DenseNet-121, were optimized by transfer learning. Model evaluation was conducted utilizing ROC analysis, accuracy, sensitivity, and specificity in relation to DEXA derived osteoporosis classifications. The optimal model, utilizing a fine-tuned DenseNet-121, attained an AUC of 0.95 and an accuracy of 91.2. [8].

In 2023, Pan *et al.* Executed a pioneering study designed to facilitate opportunistic osteoporosis screening by amalgamating imaging and clinical data via a DCNN architecture. The primary objective was to investigate if the integration of radiographic image features with clinical factors may enhance diagnostic accuracy in comparison to image-only models when evaluated against DEXA standards. The process entailed the automatic extraction of spinal ROI from standard chest or opportunistic CT scans, succeeded by feature encoding utilizing CNN architectures like ResNet and DenseNet. The collected picture features were subsequently integrated with patient-level clinical factors (e.g., age, sex, BMI, and medical history) using a late-fusion classifier head, resulting in a multi-feature prediction model. The evaluation of model performance utilized essential parameters such as AUC, sensitivity, and specificity in relation to DEXA defined osteoporosis state. The findings indicated that the fusion model markedly surpassed imaging-only baselines, with an AUC of 0.88 and a sensitivity of 85%, in contrast to 0.81 and 77% for image-only networks. [9].

In 2024, Dhanagopal et al. Intended to enhance automated osteoporosis detection from DEXA images in 2024 by the utilization of sophisticated deep learning methodologies. They employed transfer learning with a channel-boosted CNN to extract additional features from bone areas while utilizing reduced training data. The model underwent training and evaluation using DEXA datasets, achieving a sensitivity of 0.88, a specificity of 0.90, and an overall accuracy of 89%. This surpassed both baseline machine learning and conventional CNN techniques. The results indicate that integrating transfer learning with channel-boosting significantly enhances AI's capability to detect osteoporosis in DEXA images [10].

In 2024, Siddiqua A. Designed to provide a resilient computer-aided system for the automatic diagnosis of osteoporosis exploiting DEXA pictures through a transfer-learning framework integrated with

Hybrid Framework between

a U-Net–based segmentation architecture. The process commenced with the segmentation of bone regions of interest from the DEXA scans via the U-Net network, facilitating accurate extraction of pertinent structural information while minimizing background noise and extraneous anatomical regions. The segmented features were subsequently input into a transfer-learning classifier to assess BMD and T-scores, enabling precise categorization of normal, osteopenia, and osteoporotic conditions. The model was trained and validated using gathered DEXA datasets, attaining a classification accuracy of 90%, alongside strong sensitivity and specificity metrics, demonstrating dependable performance across various patient samples. The results underscore the efficacy of combining segmentation-driven feature extraction with transfer learning, illustrating that these AI pipelines can deliver swift, precise, and clinically relevant evaluations of bone health from DEXA images, thereby aiding radiologists in diagnostic decision-making and enhancing osteoporosis screening processes [11].

In 2025, Abdullah *et al.* proposed a hybrid framework that integrates Genetic Algorithm (GA) optimization with CNN for osteoporosis diagnosis. The study addresses the limitations of conventional deep learning models by introducing an adaptive optimization mechanism for hyperparameter tuning and network configuration. The results demonstrated improved diagnostic performance, emphasizing the effectiveness of combining metaheuristic optimization techniques with deep learning models in medical imaging applications [12]

No published attempts were found where DEXA imaging datasets were used for osteoporosis diagnosis. Besides, no application of BOA exists to optimise the hyperparameters of CNN. Such gaps are filled by this study.

3. Methodology

3.1 Proposed Approach

The proposed BOCNN model for classification of MLSI dataset into normal and osteoporotic classes. The process consists of a CNN model with a given architecture and the BOA for optimising hyperparameters such as the number of filters, convolutional kernel sizes, convolutional kernel strides, pooling block sizes, pooling block strides, number of dense neurones, and dropout rates. Properly tuning

Hybrid Framework between

hyperparameters improves accuracy and reduces overfitting and improves the generalisation of the model [13][14]. Figure 3 illustrate the whole framework of the suggested method.

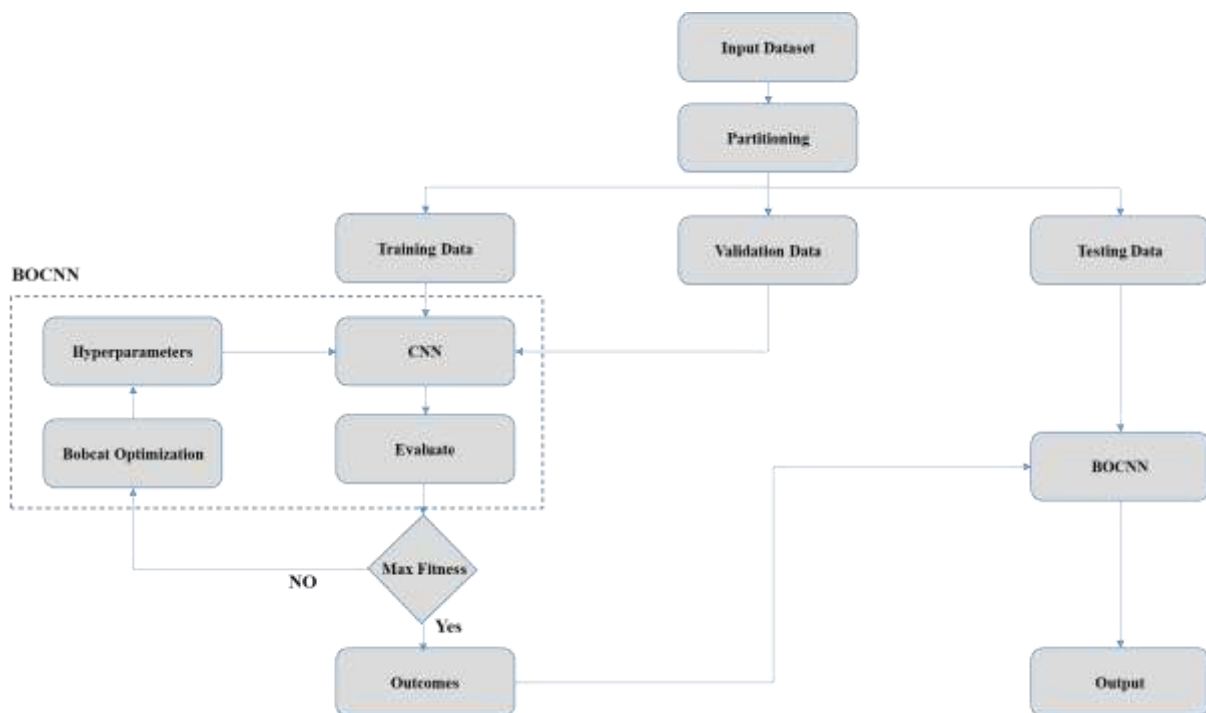


Figure 3: Block diagram of the proposed work

“The dataset of images runs as the input. Subsequently, it is partitioned into training, validation and testing groups of 60%, 20% and 20%, respectively. Consequently, we construct a CNN and initialize its hyperparameters. The BOA is employed to fine-tune hyperparameters and achieve the optimal configuration. We refer to this as the BOCNN, which subsequently tested to acquire the assessed accuracy”.

3.2 CNN Fundamentals

The input layer of a CNN receives images. Each image is of the colored type (Red, Green, and Blue (RGB)). The inputs consist of colored images, each including three RGB channels.

“The convolutional layer constitutes the essential physical mechanism in the CNN. Two-Dimensional (2D) convolution procedures must be performed for each input channel. This layer consists of a collection of image channels referred to as feature maps (or filters). The convolutional layer is crucial

Hybrid Framework between

for extracting various features from a 2D channel [15]. The process involves convolving a kernel with a channel of image. The convolution function is represented by the following equation:

$$Z(x, y) = \sum_{m=1}^M \sum_{n=1}^N R(m, n) \times W(x - m, y - n) \quad (1)$$

where $Z(x, y)$ symbolizes a computed convolution, M and N respectively refer to the width and height of the 2D input channel, $R(m, n)$ represents the input channel, and $W(x - m, y - n)$ is weight value [16].

The multiple layers also use ReLU as it is a well-known transfer function in the DL. The ReLU transfer function maintains the positive values and discards the negative values of any preceding channel (feature map). Therefore, it allows non-linear calculations. The ReLU activation function is given by the following equation:

$$ReLU(x, y) = \max(0, (x, y)) \quad (2)$$

where $ReLU(x, y)$ represents a computed ReLU, and $\max$ is the maximum operation [16].

“The pooling layer reduces the sizes of received channels, resulting in small sized feature maps. It is typically implemented in one of two types: max pooling or average pooling. Its advantage is reducing the spatial dimensions of feature maps while preserving the most prominent characteristics. The computation of maximum pooling is executed in accordance with the below equation:

$$K(i, j) = \max(\mathbf{V}) \quad (3)$$

where $K(i, j)$ is a computed pooling and $\mathbf{V}$ is a small matrix (block) in a previous channel [15].

The Fully connected layer, also known as dense layer, is carried out after the feature extraction part. It comprises of many neurons, every neuron in this layer is connected to all neurons in a previous layer. The number of neurons in FC layer can be equal to the number of required outputs of classes (C). The essential equation in FC layer can be illustrated as follows”:

$$FC(c) = \sum_{l=1}^p (FW(c, l) \times P(l)) + B(c) \quad (4)$$

where $FC(c)$ mean the calculated value in the fully connected layer, c illustrate the neuron's number in the current layer, P shows the number of neurons in the previous layer, $FW(c, l)$ represents a connection weight value between the previous and current layers and $B(c)$ represents a bias value [16].

A softmax layer provides the related probabilities for each output class accordingly to the provided input, such probabilities sum up to one. This layer basically uses the softmax activation function. The general equation in the softmax layer can be given as follows:

$$S(c) = \frac{\exp(FC(c))}{\sum_{l=1}^C \exp(FC(l))} \quad (5)$$

where $S(c)$ shows the calculated softmax value and $\exp$ is the exponential [17].

3.2 BOA Fundamentals

“The BOA is a recently established nature-inspired metaheuristic algorithm, proposed in 2024. It mimics the distinctive hunting technique of bobcats in their natural habitat. It aims to tackle intricate optimization challenges by efficiently balancing between the exploration and exploitation. The two phases of this algorithm make it unique. These are the exploration and exploitation phases. The exploration phase mimics the bobcat's strategy in stealthily tracking a prey over a wide area. The exploitation phase represents a precise and aggressive chase to catch the prey. This bio-inspired dual phases mechanism allows BOA to search globally while efficiently and rapidly converging toward the optimal solution [18]”.

“In our study we utilize the BOA to optimize the hyperparameters of CNN to achieve a maximum performance. The algorithm initiates with a set of candidate solutions (bobcats) that are randomly scattered throughout the searching space, each one of them represents a potential solution to the optimization problem. The fitness of each candidate is evaluated iteratively, increasingly guiding the population toward the optimal region of searching space. As mentioned, the algorithm process is structured into two main phases that reflects the natural hunting behavior of bobcats [18]. In more details”:

The exploration Phase (Tracking the Prey): In this phase, bobcats survey the searching area broadly, simulating to their behavior when tracking a prey. The algorithm promotes diversity by allowing bobcats' candidates to move towards randomly selected positions. This prevents premature convergence and ensures comprehensive exploration of the solution space. This phase is essential for pinpointing the prospective area inside the search space [18].

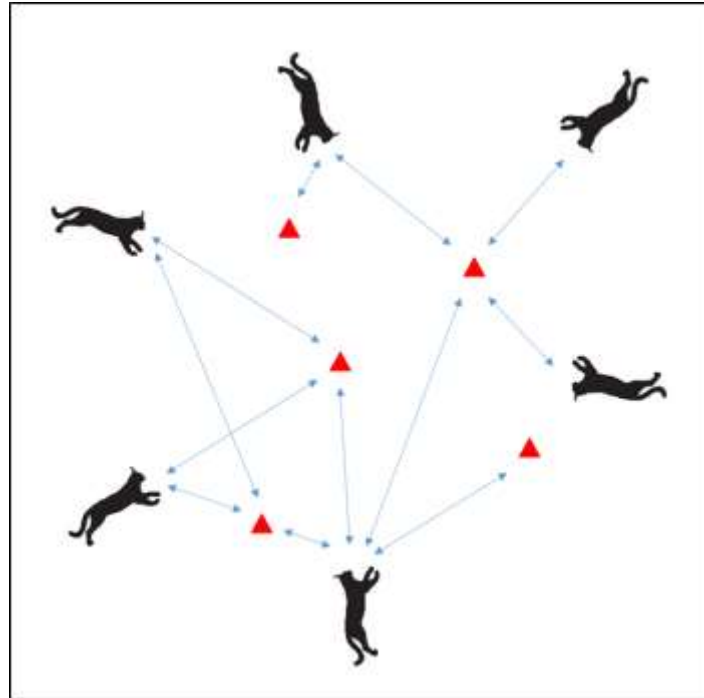


Figure 4: Conceptual depiction of the BOA exploration phase, wherein bobcats traverse randomly towards several candidate solutions, hence providing diversity throughout the search space.

The Exploitation Phase (Chasing the Prey): Upon identifying the promising area, the algorithm transitions to this phase, designated for pursuit behavior. In this case, bobcats change their positions based on the best solutions they've got so far, making their search more focused on finding the best solution. This targeted enhancement guarantees that the algorithm efficiently advances candidate solutions and approaches the optimal solution [18].

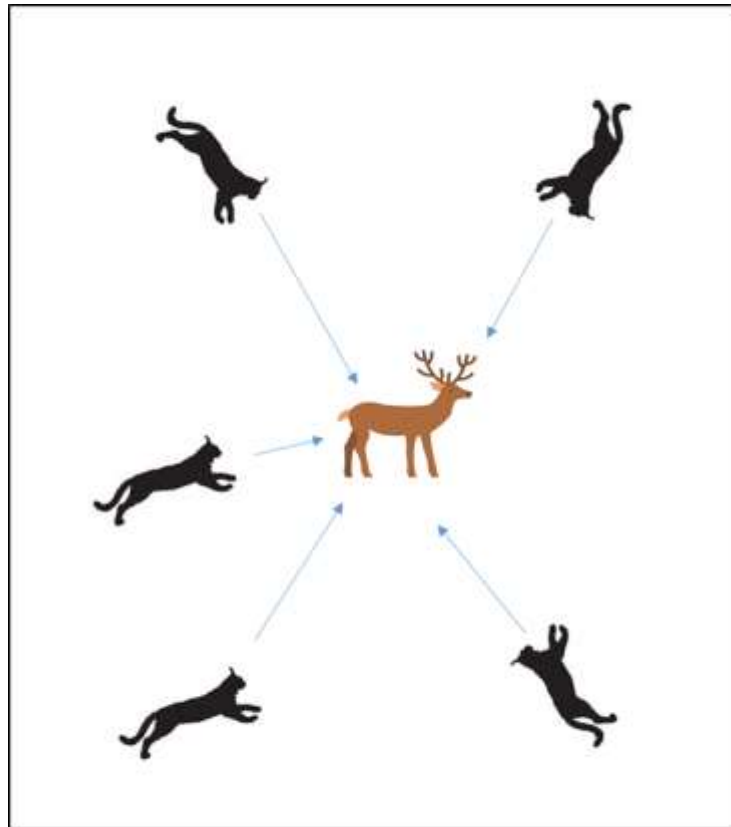


Figure 5: Demonstration for the convergence of bobcats toward the optimal solution

“BOA is different from other metaheuristic algorithms accordingly to how it was inspired and how it works. The following main points illustrate the distinctive aspects of BOA's biological modelling, search technique, and adaptive behavior in comparison to other algorithms [18]:

- Exceptional biological inspiration: BOA is different from other metaheuristics like WOA and GA because it is based on its uniqueness in goal-driven hunting behavior. It focusses on how predators of bobcats interact with each other toward the prey. Each candidate solution mimics a bobcat that explores its environment independently, then switches to exploitation by simulating a targeted chase toward the best-found prey. This biologically faithful modeling introduces a novel structure for balancing exploration and exploitation in optimization problems.
 - Dual phases search mechanism: BOA delineates a definite separation between the periods of exploration and exploitation. It entails a systematic search procedure, improved capacity to evade local optima, and a maintained equilibrium between global and local searches.

- Adaptive behavior: BOA demonstrates adaptive search dynamics by modifying its movement according on the prevailing distribution and fitness of candidate solutions. This capability to respond enables the algorithm to alternate between exploration and exploitation, facilitating proximity to optimal solutions while mitigating the risk of premature stagnation.

It has been cited that empirical assessments have confirmed BOA capability. Particularly, in solving complex optimization problems. That is, it surpasses many well-known metaheuristic algorithms, while maintaining a good balance between exploration and exploitation”.

3.3 Integrating between CNN and BOA

The BOCNN model is proposed as discussed earlier. BOA is used in the two phases of tracking for prey then chasing it for the best solution which means the best optimised hyperparameters set of CNN. “For BOA ranking the quality of possible solutions, it critically depends on the provided objective function. The fitness function could vary depending on the specific application, such as maximizing accuracy or minimizing error in AI tasks. The fitness function is used to evaluate the model's performance during the optimization process. In this study, it is suggested to combine both training and validation accuracies to facilitate the balance of the model's generalization. It is constructed as a weighted aggregation of training accuracy and validation accuracy. This weighting system emphasizes the model's proficiency in learning from training data while also accounting for its generalization abilities on validation data. The inclusion of validation accuracy aids in reducing the likelihood of overfitting. The fitness function of the WOCNN can be illustrated by the following equation:

$$F = (\alpha \times TA) + (\beta \times VA) \quad (6)$$

where F represents the fitness function, α and β represent variable factors as $(\alpha + \beta = 1)$, TA represents the training accuracy, and VA represents the validation accuracy.

The training accuracy metric evaluates the model's learning from the training data, whereas validation accuracy measures the model's generalization to unseen data throughout the training process [19]. To find the best CNN-optimizing hyperparameters, BOA looks at 18 of them, such as convolutional filter numbers, convolutional kernel size, convolutional kernel stride, pooling size, pooling block stride, dense neuron numbers, and dropping rates. Hyperparameters optimization can

Hybrid Framework between

enhance convergence speed, reduce training duration and lower computing expenses [20]". Such proposed optimization can improve predictive performance and provide more efficient model for osteoporosis diagnosis.

4. Results and Discussions

4.1 Employed Dataset

This dataset is usually known as MLSI. Diagnosis of osteoporosis is acquired by the DEXA scan. Contains 211 lumbar spine pictures. The dataset includes images cropped from the DEXA display monitor, with the approximate size of $453 \times 519 \times 3$ pixels. All images are in the Joint Photographic Experts Group (JPEG) format. The images were collected and validated at Dr. Khalid Ghanim Majeed's private clinic in Mosul, Iraq. The dataset is divided into osteoporotic and normal cases according to the BMD measurement.

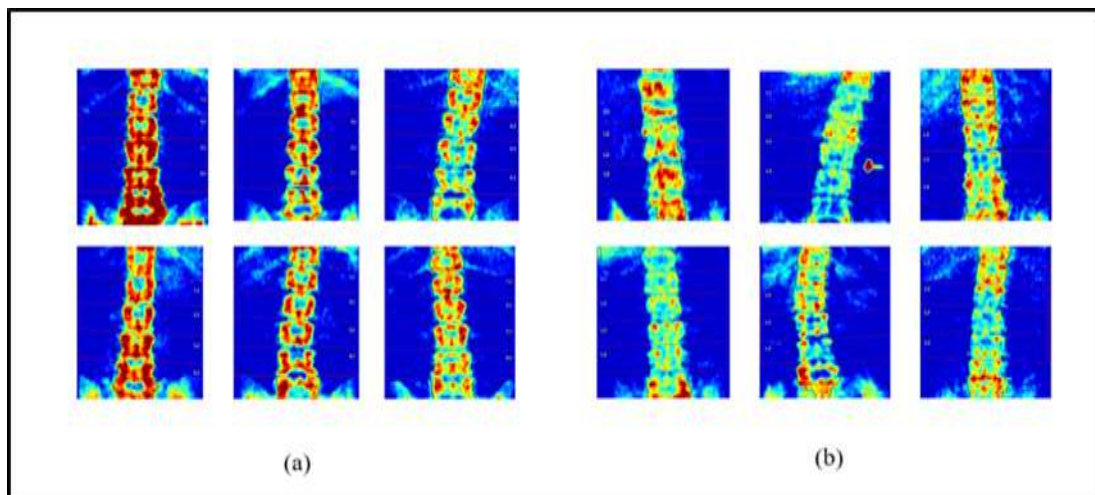


Figure 6: MLS Diverse Images from dataset (a) Normal (b) Osteoporotic

4.2 Standardizations

The MLSI dataset has 126 training images, 42 validation images, and 43 testing images, for a total of 211 images in three categories. All images are normalised to the size of $128 \times 128 \times 3$. To improve the network's performance and to avoid overfitting, we increased the number of training and validation

images. Augmentation operations: rescaling, shearing by a factor of 0.2, zooming by a factor of 0.2, and horizontal flipping. They have been used to provide insight into the diversity between the images offered.

All experiments were performed on a laptop computer with the following specifications: The Lenovo laptop features an Intel core i5 processor running at 2.20 GHz and comes with 12 GB of RAM. Code has been executed online via google Colab platform by activating Pro Pulse version with Python programming language version 3.9. and a Central processing unit (CPU) with a maximum of 51 gigabytes of Random Access Memory (RAM).

4.3 BOA Optimization

As previously mentioned, the proposed BOCNN model utilize BOA to optimize CNN hyperparameters. Figure 7 shows the development of fitness score curve over iterations.

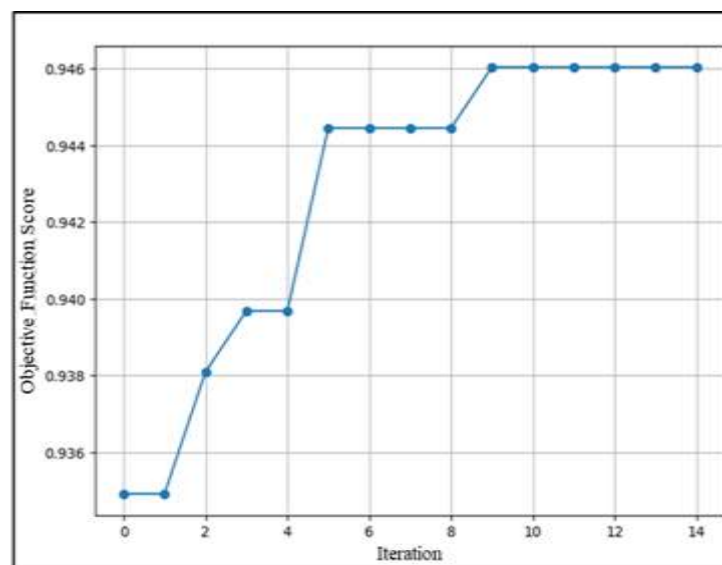


Figure 7: Development of fitness score curve over iterations

This figure demonstrates the progression of the best fitness score over 15 generations during the BOA hyperparameter tuning process. Initially, the fitness score is relatively low, starting at approximately 0.935. Nonetheless, it advances swiftly inside the initial generations, demonstrating the algorithm's capacity to promptly discern more advantageous choices. From the 2nd to the 5th generations, the enhancement progresses consistently, indicating that BOA is effectively optimizing its search within a

Hybrid Framework between

constrained solution space. Between the 6th and 8th generations, the rate of enhancement diminishes, signifying that the algorithm is shifting from exploration to fine-tuning, implementing incremental modifications to optimize performance. The curve reaches its apex at the 9th generation with a fitness score about 0.946 and maintains stability until the 14th generation. This plateau indicates the approach towards an ideal or near-optimal solution. The graphic illustrates BOA's ability to reconcile global search with local exploitation, showcasing its efficacy in optimizing hyperparameters to improve model performance.

4.4 BOCNN Specifications

After several experiments the proposed CNN model for classification of the MLIS images into normal and osteoporosis cases. It has 11 layers architecture that extracts and classifies osteoporosis features systematically. The layers are input layer, first convolution layer, first pooling layer, second convolution layer, second pooling layer, third convolution layer, third pooling layer, flatten layer, first dense layer, second dense layer and softmax layer. BOA optimises 18 hyperparameters for the BOCNN, which are located in the CNN main layers of convolution, pooling and dense, where all such layers are considered. Each convolution layer has the parameters such as number of filters, kernel size and kernel stride. The parameters of any pooling layer are: block size, block stride. The parameters in each dense layer are the number of neurones and the dropout rate. Table 1 summarises the 18 hyperparameters and their initial setup BOA values.

“Table 1: The examined CNN hyperparameters along with their initial value configurations (search space)

Index	Hyperparameter	Initial Value	Type
1	Number of filters in layer 1	Between 32 to 256	Random Integer
2	Kernel size in layer 1	3, 4 or 5	Random choice
3	Kernel stride in layer 1	1 or 2	Random choice
4	Block size in layer 2	2, 3 or 4	Random choice
5	Block stride in layer 2	1 or 2	Random choice
6	Number of filters in layer 3	Between 32 to 256	Random Integer
7	Kernel size in layer 3	3, 4 or 5	Random choice
8	Kernel stride in layer 3	1 or 2	Random choice

Hybrid Framework between

9	Block size in layer 4	2, 3 or 4	Random choice
10	Block stride in layer 4	1 or 2	Random choice
11	Number of filters in layer 5	Between 32 to 256	Random Integer
12	Kernel size in layer 5	3, 4 or 5	Random choice
13	Kernel stride in layer 5	1 or 2	Random choice
14	Block size in layer 6	2, 3 or 4	Random choice
15	Block stride in layer 6	1 or 2	Random choice
16	Number of dense neurons in layer 7	Between 64 to 512	Random Integer
17	Number of dense neurons in layer 8	Between 64 to 512	Random Integer
18	Dropout rate in layers 7 and 8	Between 0.1 to 0.5	Random float"

The best hyperparameters are selected by the maximum fitness value. Fig. 8 shows the final BOCNN design, it has the best values achieved for the 18 hyperparameters. For the first convolutional layer, the number of filters is 79 filters, the kernel size is 5×5 pixels and the stride is 2×2 pixels. First pooling layer: block size = 3×3 pixels, stride = 2×2 pixels. For second convolution layer, number of filters = 163 filters, kernel size = 5×5 pixels and stride = 1×1 pixel. The block size of the second pooling layer is 4×4 and the stride is 1×1 pixels. The number of filters for the third convolution layer is 125 filters with kernel size 5×5 pixels and stride 2×2 pixels. For the third pooling layer, block size = 3×3 pixels, stride = 1×1 pixels. Dense layer 1: no. of neurones = 226 nodes, dropout = 0.3. For second dense layer # of neurones = 286 nodes and dropout = 0.3.

Hybrid Framework between

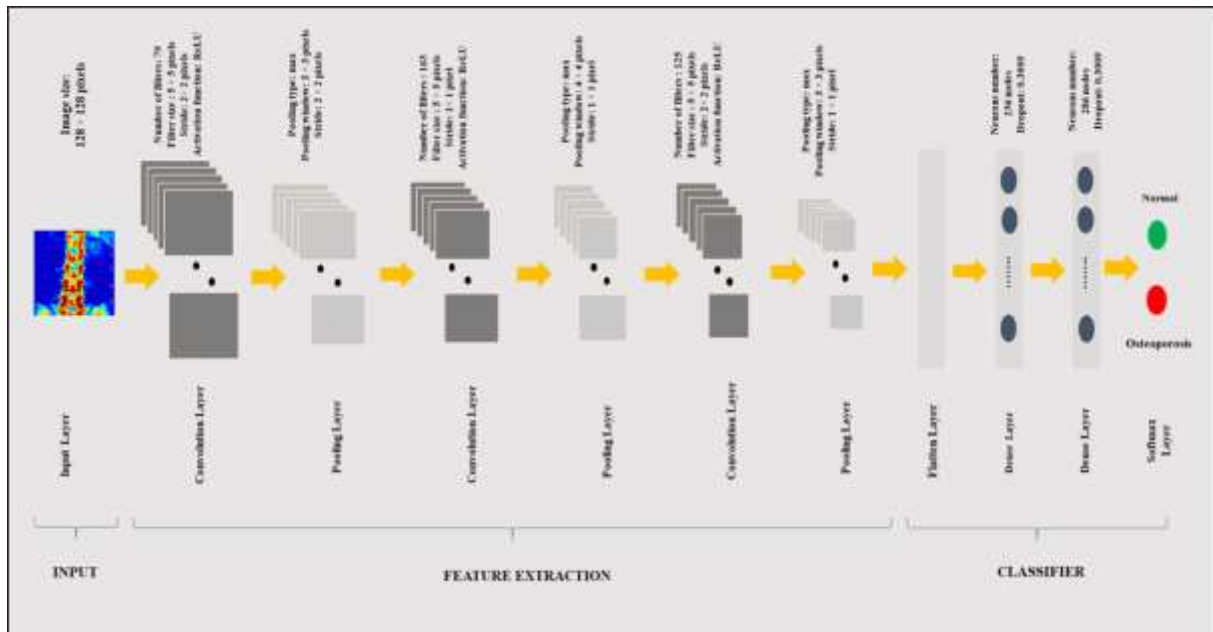


Figure 8: full architecture of the proposed BOCNN model

4.5 BOCNN Training and Validation

The BOCNN is then trained with the optimal hyperparameters values found. The training settings are as following: ADAM optimiser, learning rate 0.001, batch size 32, max pooling window, ReLU activation function, same padding, maximum 60 epochs, early termination if validation loss does not improve over 5 epochs. Watch the validation loss to save time and avoid overfitting.

Figure 9, part A, presents the training and validation accuracy curves of the model over 40 epochs. During the early stages (epoch 0 to 5), there is a significant rise in training accuracy, suggesting that the model quickly starts to grasp patterns from the training data. The validation accuracy shows a similar rising trend, although it is characterized by notable oscillations that reflect heterogeneity in the model's generalization performance. As training progresses beyond epoch 10, both curves generally ascend, with training accuracy stabilizing above 0.90. The validation accuracy exhibits oscillations during training but remains close to the training accuracy, indicating a well-balanced learning process marked by adequate generalization and minimal overfitting.

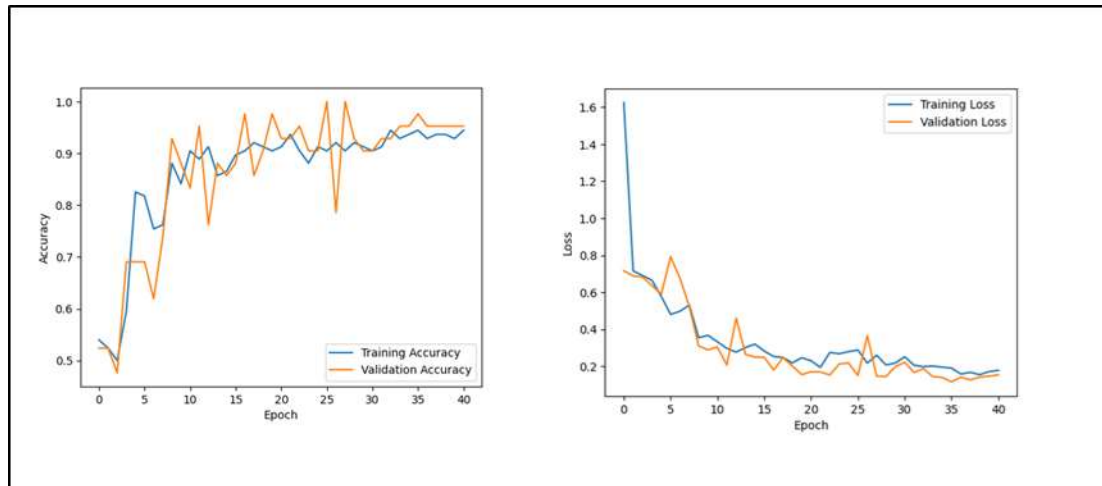


Figure 4.9: Graphs depicting the training and validation phases of the BOCNN model. The accuracies' training and validation curves are displayed on the left, while the losses' training and validation curves are presented on the right.

Part B of the Figure 4.9 depicts the paths of training and validation loss. The training loss commences at a significantly high level and declines rapidly in the initial epochs, signifying effective early learning. The validation loss demonstrates a significant decline during this phase and maintains a consistent downward trend, ultimately stabilizing at a low range in the subsequent epochs. Intermittent small increases in validation loss could indicate a temporary responsiveness to validation samples or slight overfitting; however, the general trend stays consistent. Collectively, these curves illustrate the model's ability to learn efficiently from the data while preserving generalization performance over the course of the training period.

4.6 GOCNN Testing

Finally, the testing phase of BOCNN model has exploited unexplored data of MLSI dataset. Figure 9 shows the confusion matrix for the model's performance on test data for the normal and osteoporotic classes. The model properly identifies 20 instances as normal and 21 cases as osteoporosis. However, it has misclassified two normal cases. This results in a recall of 91%. The accuracy for osteoporosis detection has achieved the exact proportion of 100%, which means every anticipated osteoporosis is right. The overall accuracy has been benchmarked to be 95%, which shows that our proposed BOCNN model can identify well between normal and osteoporotic cases for real clinical data. The high findings suggest that

Hybrid Framework between

the BOCNN is learning important patterns from the training data and is able to confidently detect the presence or absence of osteoporosis.

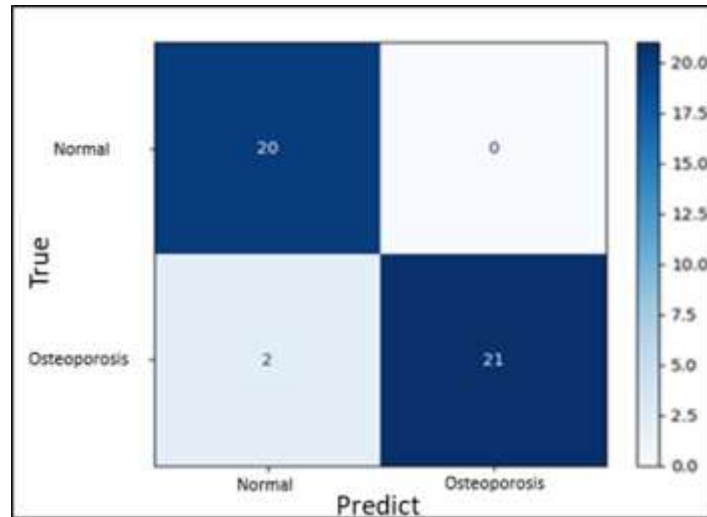


Figure 10: Confusion matrix for the WOCNN testing phase

The ROC curve shows the trade-off between the true positive rate (sensitivity) and the false positive rate across different classification thresholds. Both classes achieve an impressive AUC score of 0.98, indicating outstanding discriminatory power.

The ROC curve for the "normal" class, shown in blue, rises sharply towards the upper-left corner, demonstrating that the model correctly identifies a high proportion of true negatives and true positives with minimal false positives. Similarly, the red curve for the "osteoporosis" class follows a comparable trajectory, also approaching the ideal point (0,1), which denotes perfect classification

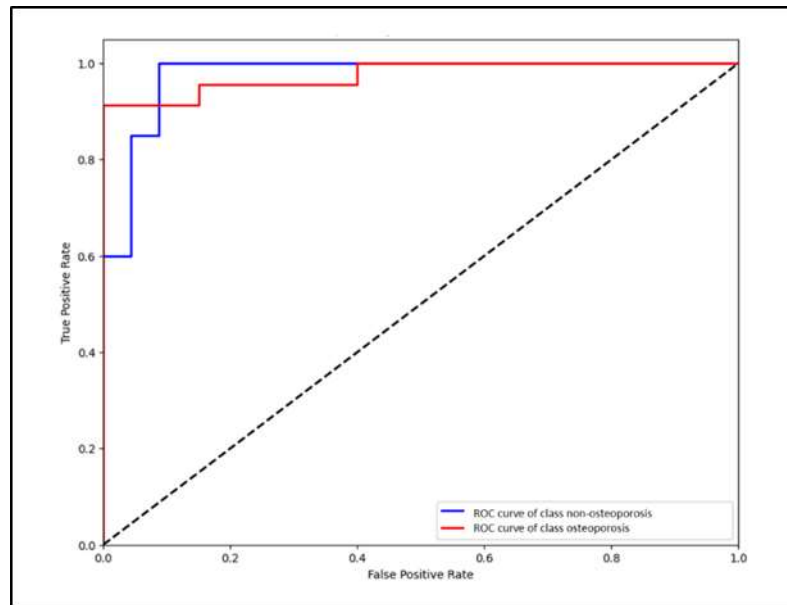


Figure 10: The ROC curve for normal and osteoporosis classifications

This result shows that the BOCNN model has achieved very high accuracy in the diagnosis of osteoporosis, which may contribute much to the early detection and intervention strategies of osteoporosis. Moreover, it can help evaluate the progress of treatment for patients, thus decreasing the need for manual and time-consuming evaluations.

4.7 Contrasts with alternative Models

Comparisons with other DL models are also considered in this study, they include: EfficientNet, InceptionV3, GoogleNet, MobileNet, ResNet and VGG16. All of these DL models have been trained, validated and tested for the same task and by using the same data, this ensures providing fair comparisons. Figure 11 shows the confusion metrics of testing the compared models, they can be considered as the bases of calculating the performance evaluations such as the accuracies and AUCs.

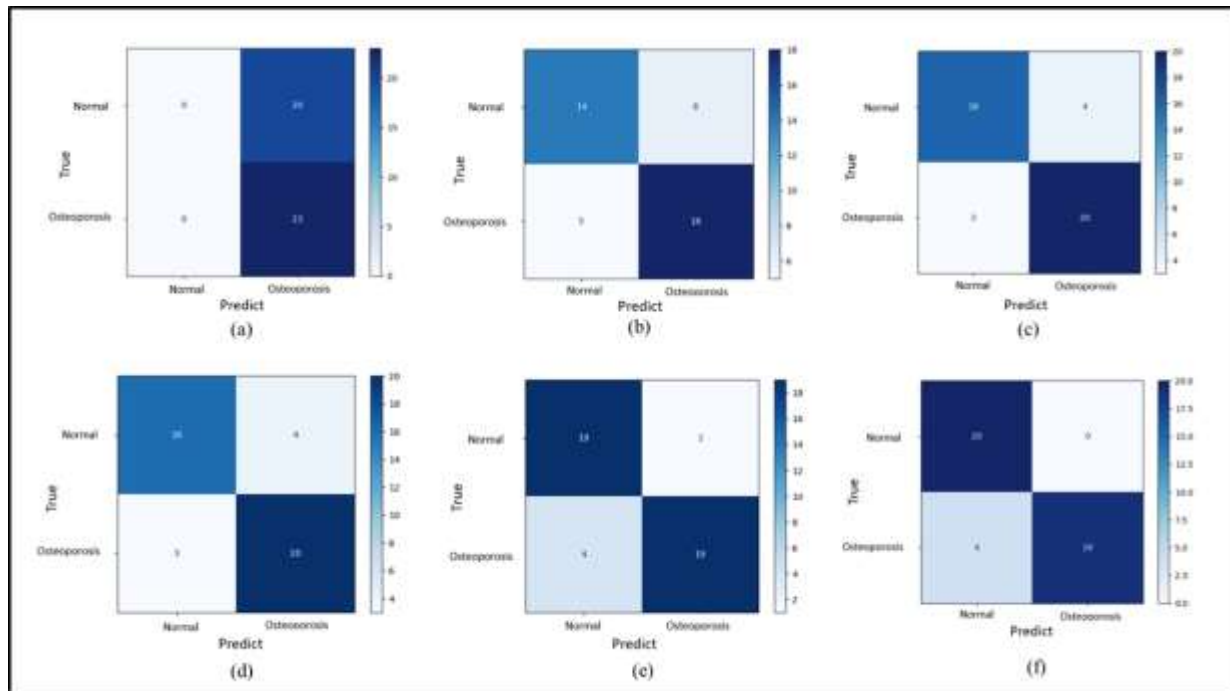


Figure 4.18: Confusion matrices of testing the compared DL models: (a) EfficientNet, (b) InceptionV3, (c) GoogleNet, (d) MobileNet, (e) ResNet and (f) VGG16

These results allow observing significant comparisons. EfficientNet attains the worst performance, with the accuracy of 53.4% and AUC of 0.60. These statistics indicate that this network has no suitable hyperparameters. InceptionV3 obtains better results, with the accuracy of 74.4% and AUC of 0.88, which can be attributed to its multi-branch architecture and slightly appropriate hyperparameters. GoogleNet and MobileNet both produce similar results, with the accuracy of 83.7% and AUC of 0.94. Such outcomes reveal that their hyperparameters are better but remain limited. ResNet achieves even better performance, with the accuracy of 88.3% and AUC of 0.93, reflecting the advantage of residual connections in mitigating vanishing gradients and improving the effects of its hyperparameters. VGG16 reaches the highest results among all previously compared DL models, with the accuracy of 90.7% and AUC of 0.94. These results confirm the capability of this DL model, however, it still lacks for the hyperparameters optimization to further enhance its performance.

5. Conclusion

In this study, we used a dataset of DEXA clinic in Mosul, Iraq from MLSI to classify the cases as normal or having osteoporosis. We introduce the BOCNN model. It shows the capability of BOA to optimize 18 hyperparameters of a CNN to achieve the maximum feasible accuracy. The results highlight

the importance of the choice of optimal values of CNN hyperparameters, since they might have a considerable impact on the acquired performance.

The MLSI dataset consists of 211 genuine clinical photos. They are separated in training, validation and testing sets. The different hyperparameters studied include the number of filters, convolutional kernel sizes, convolutional kernel strides, pooling block sizes, pooling block strides, number of dense neurones, and dropout rate. The best configuration of the suggested BOCNN model attained a very high testing accuracy of 95%. Furthermore, 0.98 AUC value is attained for each case of normal class and osteoporosis class. Accuracy is at a flawless 100%. The recall achieved an impressive 91% success rate.

References:

- [1] P. C. Kristie N. Tu, PharmD, BCPS, CGP; Janette D. Lie, PharmD, BCACP; Chew King Victoria Wan, PharmD Candidate; Madison Cameron, PharmD Candidate; Alaina G. Austel, PharmD Candidate, and Jenny K. Nguyen, "Osteoporosis: A review of treatment options," *Pharmacy and Therapeutics*, vol. 43, no. 2, pp. 92–104, 2018.
- [2] E. Michael Lewiecki, Deborah Cotton, Darren Taichman, and Sankey Williams, "In the Clinical Osteoporosis," *Annals of Internal Medicine*, vol. 155, no. 1, 2011, doi: 10.7326/0003-4819-155-1-201107050-01001.
- [3] J. A. Kanis, E. V. McCloskey, H. Johansson, N. C. Harvey, A. Oden, and F. Borgström, "European guidance for the diagnosis and management of osteoporosis in postmenopausal women," *Osteoporosis International*, vol. 31, no. 1, pp. 1–15, 2020, doi: 10.1007/s00198-019-05176-3.
- [4] R. Jang, J. H. Choi, N. Kim, J. S. Chang, P. W. Yoon, and C. H. Kim, "Prediction of osteoporosis from simple hip radiography using deep learning algorithm," *Scientific Reports*, vol. 11, no. 1, 2021, doi: 10.1038/s41598-021-99549-6.
- [5] S. Bhattacharya, D. Nair, A. Bhan, and A. Goyal, "Computer Based Automatic Detection and Classification of Osteoporosis in Bone Radiographs," in *2019 6th International Conference on Signal Processing and Integrated Networks, SPIN 2019*, 2019, pp. 1047–1052, doi:

- 10.1109/SPIN.2019.8711616.
- [6] T. T. Ho, J. G. Lee, S. J. Lee, H. Kim, and J. H. Kim, "Deep learning-based prediction of bone mineral density and osteoporosis from plain radiographs," *IEEE Access*, vol. 8, pp. 142402–142412, 2020, doi: 10.1109/ACCESS.2020.3013795..
 - [7] Y. Zhang, H. Wang, L. Xu, and Q. Li, "Deep learning-based classification of osteoporosis using lumbar spine radiographs," *Osteoporosis International*, vol. 33, no. 5, pp. 1125–1134, 2022, doi: 10.1007/s00198-021-06171-7.
 - [8] R. Jang, J. H. Choi, N. Kim, J. S. Chang, P. W. Yoon, and C. H. Kim, "Prediction of osteoporosis from simple hip radiography using deep learning algorithm," *Scientific Reports*, vol. 11, no. 1, 2021, doi: 10.1038/s41598-021-99549-6.
 - [9] J. Pan, P.-C. Lin, S.-C. Gong, Z. Wang, R. Cao, Y. Lv, K. Zhang, and L. Wang, "Effectiveness of opportunistic osteoporosis screening on chest CT using a deep convolutional neural network model," *Scientific Reports*, vol. 14, 2024.
 - [10] R. Dhanagopal, R. Menaka, R. Suresh Kumar, P. T. Vasanth Raj, E. L. Debrah, and K. Pradeep, "Channel-boosted and transfer learning convolutional neural network-based osteoporosis detection from CT scan, dual X-ray, and X-ray images," *Computational Intelligence and Neuroscience*, vol. 2024, Article ID 3733705, 2024, doi: 10.1155/2024/3733705.
 - [11] A. Siddiqua, "Automated osteoporosis diagnosis from DEXA images using U-Net and transfer learning," *arXiv preprint arXiv:2412.09330*, 2024.
 - [12] A. K. Abdullah, R. R. O. Al-Nima, and K. G. Majeed, "Accurate osteoporosis diagnosis model proposing genetic algorithm optimization for convolutional neural network," *Proceedings of the 2nd International Conference on Sustainable Development Techniques (ICSdT2025)*, vol. 5, no. 1, 2025, doi: 10.56286/jc6qnd62.
 - [13] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
 - [14] J. Bergstra and Y. Bengio, "Random search for hyper-parameter optimization," *Journal of Machine Learning Research*, vol. 13, pp. 281–305, 2012.

- [15] Ahmed Saeed Ibrahim Al-Obaidi, Raid Rafi Omar Al-Nima, and Tingting Han, “Interpreting arabic signal phabet by using the deep learning,” in *AIP Confonfrence Proceedings*, vol. 2862, 2023, doi: 10.1063/5.0171428.
- [16] Saad Albawi, Tareq Abed Mohammed, and Saad Al-Zawi, “Understanding of a convolutional neural network,” *Proceedings of 2017 International Conference on Engineering and Technology*,. pp. 1–6, 2017, doi: 10.1109/ICEngTechnol.2017.8308186.
- [17] H. Wu and J. Zhao, “Deep convolutional neural network model based chemical process fault diagnosis,” *Computers and Chemical Engineering*, vol. 115. pp. 185–197, 2018, doi: 10.1016/j.compchemeng.2018.04.009.
- [18] Z. Benmamoun, K. Khlie, and B. Gulnara, “Bobcat optimization algorithm: An effective bio-inspired metaheuristic algorithm for solving supply chain optimization problems,” *Scientific Reports*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-70497-1.
- [19] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, , *Deep Learning*. MIT Press, 2016.
- [20] Lisha Li, Kevin Jamieson, Giulia DeSalvo, Afshin Rostamizadeh, and Ameet Talwalkar, “Hyperband: A novel bandit-based approach to hyperparameter optimization,” *Journal of Machine Learning Research*, vol. 18, no. 1, pp. 1–52, 2018.