

二国間交流事業 共同研究報告書

令和6年4月1日

独立行政法人日本学術振興会理事長 殿

[日本側代表者所属機関・部局]
九州大学大学院・システム情報科学研究院
[職・氏名]
教授・櫻井 幸一
[課題番号]
JPJSBP 120227718

1. 事業名 相手国: インド (振興会対応機関: DST) との共同研究

2. 研究課題名

敵対的攻撃に対する深層学習能力の限界解明とそのサイバーセキュリティへの応用

(英文) Investigation of power of Deep Neural Networks against various adversarial attacks
and their applications to Cybersecurity

3. 共同研究実施期間 2022 年 6 月 1 日 ~ 2024 年 3 月 31 日 (1 年 10 ヶ月)【延長前】 年 月 日 ~ 年 月 日 (年 ヶ月)

4. 相手国側代表者(所属機関名・職名・氏名【全て英文】)

Indian Institute of Information Technology, Design and Manufacturing.
Jabalpur • Assistant Professor • Sraban Kumar Mohanty

5. 委託費総額(返還額を除く)

本事業により執行した委託費総額		1,686,351 円
内訳	1年度目執行経費	950,000- 円
	2年度目執行経費	736,351- 円
	3年度目執行経費	*****- 円

6. 共同研究実施期間を通じた参加者数(代表者を含む)

日本側参加者等	6 名
相手国側参加者等	3 名

* 参加者リスト(様式 B1(1))に表示される合計数を転記してください(途中で不参加となった方も含め、全ての期間で参加した通算の参加者数となります)。

7. 派遣・受入実績

	派遣		受入
	相手国	第三国	
1 年度目	0	0	0(0)
2 年度目	0	0	2 (2)
3 年度目	***	***	***(***)

* 派遣・受入実績(様式 B1(3))に表示される合計数を転記してください。

派遣:委託費を使用した日本側参加者等の相手国及び相手国以外への渡航実績(延べ人数)。

受入:相手国側参加者等の来日実績(延べ人数)。カッコ内は委託費で滞在費等を負担した内数。

8. 研究交流の概要・成果等

(1)研究交流概要(全期間を通じた研究交流の目的・実施状況)

主題である、敵対的攻撃に対する深層学習とそのサイバーセキュリティへの応用に関しては、日本側が先行しており、今回の国際共同研究の結果、インド側研究者は新しい知見を得られたと評価している。

逆に、インド側は、医療関係への機械学習アルゴリズムの応用に関して精通しており、これに関しては、日本側は、学ぶところ大であった。

初年度は、コロナやインド側予算配分の遅れなどの障害で対面での交流は実現しなかったが、online/emailでの研究会議と討論で、共同研究を遂行した。2年目の冬には、インド側予算も確保でき、日本側への訪問滞在も実現できた。

(2)学術的価値(本研究交流により得られた新たな知見や概念の展開等、学術的成果)

2件の共著ジャーナル論文を、発表できたのは、最大の成果である:

[2a] Ishak Meraouche, Sabyasachi Dutta, **Sraban Kumar Mohanty**, Isaac Agudo, **Kouichi Sakurai**.

Learning Multi-Party Adversarial Encryption and Its Application to Secret Sharing. IEEE Access 10: 121329–121339 (2022)

本研究は、日本側研究室博士学生であった第一著者(国費留学生)の学位論文の主題であった深層学習を使った暗号システムの設計と評価に関する研究である。

[2b] Surbhi Soni, **Ayan Seal**, **Sraban Kumar Mohanty**, **Kouichi Sakurai**.

Electroencephalography signals-based sparse networks integration using a fuzzy ensemble technique for depression detection. Biomed. Signal Process. Control. 85: 104873 (2023)

本研究は、インド側主導の医療治療情報系に機械学習での解析を駆使する研究であり、第一著者のインド側学生の研究論文に、日本側 PI が研究コメントした成果である。インド側は、深層学習を初め、機械学習の応用先に、医療系が先行していることを、今回の国際共同研究で知る機会を得た。

(3)相手国との交流(両国の研究者が協力して学術交流することによって得られた成果)

双方の得意/強みの関係と違いを、共同研究で理解し、お互いに補完できた。

インド側 PI は、クラスター分類型機械学習アルゴリズムに精通し、敵対的攻撃に対する深層学習の応用に関しては、日本側が先行していた。論文作成にあたっては、インド側が画像認識への応用に関する研究草案を作成し、共同研究のきっかけとした。博士学生/日本側が専門家の立場から技術コメントし、最終的には共著論文として、ジャーナル論文誌へ投稿できた。

(4)社会的貢献(社会の基盤となる文化の継承と発展、社会生活の質の改善、現代的諸問題の克服と解決に資する等の社会的貢献はどのようにあったか)

インド PI の Mohanty は、以前にも九大に招聘したことがあったが、同僚の Ayan Seal は、日本滞在自体が今回初めてということで、貴重な機会を提供できたと評価している。

日本側 PI の櫻井は、インド側研究機関には、コロナ以前に過去数回滞在したことがある。ジャバルプールの町自体は、空港の国際化など確実に発展している話も、今回のインド側研究員受け入れ期間中に直接話を聞く機会を得た。また、インド側機関は、学生数も増えて拡大している反面、教員の数は増えないままの拡張に関する

課題なども意見交換できた。

(5)若手研究者養成への貢献(若手研究者養成への取組、成果)

日本側は、博士課程の学生(国費)が、インド側との共著ジャーナル論文を1つの成果として、博士号を取得で、現在はエンジニアとして日本企業で勤務している。

また、日本側の修士課程学生が、インド側研究者が九大に滞在中に、大規模言語モデルに関する研究を紹介し、意見交換を行う機会も貴重であった。この研究は、日本側 PI が、3 月のセキュリティ研究会で発表した。

また、連合学習を研究している博士学生のジャーナル論文草案には、インド側研究者よりコメントを受けて、共著論文として現在投稿中である。

(6)将来発展可能性(本事業を実施したことにより、今後どのような発展の可能性が認められるか)

インド側は、DST の予算措置が遅れたため、あと一年間は、本研究プロジェクトを継続できる。日本側で受け入れ滞在研究費を確保できたならば、2024 年度も招聘を検討したい。

また、共同研究成果の一部は、論文化し、現在投稿中や、これから投稿予定のものもあり、本 JSPS-DST プロジェクトが終了して以降も、論文発表へ向けて、共同研究討論を、電子メールや online 会議で続ける。

(7)その他(上記(2)～(6)以外に得られた成果があれば記載してください)

例:大学間協定の締結、他事業への展開、受賞など

インドとの国際共同研究は、今回の IIIT, Design and Manufacturing, Jabalpur 校以外に、複数機関と継続/進行しており、機会をみて、他の国際共同研究事業へも展開したい。