N. 1 posto – **Rif. 1**

Progetto: "Supporting Project to Restart on Intelligent Networks for Telecommunications" (SPRINT) (cascade call PNRR del progetto NetwWin di RESTART – Spoke 8)

CUP: E83C22004640001

Dipartimento: Ingegneria dell'Informazione e Scienze Matematiche - DIISM

Gruppo disciplinare: 09/IINF-03 Telecomunicazioni

Settore/i scientifico disciplinare/e: IINF-03/A Telecomunicazioni

Durata e tipo contratto: Triennale – Tempo pieno

Campo: Engineering

Oggetto del contratto: Progetto "Supporting Project to Restart on Intelligent Networks for Telecommunications" (SPRINT) (cascade call PNRR del progetto NetwWin di RESTART – Spoke 8). Titolo della linea di ricerca di base alla quale è collegato il contratto: "Inference and learning over networks, intelligent services and sensing using swarms of aerial vehicles and UAV-assisted networks" (WP3).

Obiettivi di produttività: Nell'arco di attività del progetto è prevista la partecipazione ad almeno due convegni per presentare i risultati della ricerca e la pubblicazione di almeno un lavoro su rivista internazionale. Per quanto concerne i diritti, i doveri e le modalità di svolgimento dell'attività si rinvia al Regolamento per i ricercatori a tempo determinato L. 240/2010 (D.R. 1891/2018).

Titolo attività ricerca (ITA): "Sistema mobile per la raccolta di dati IoT tramite droni ed elaborazione a bordo"

Descrizione sintetica dell'attività di ricerca (ITA): L'obiettivo principale è quello di sviluppare algoritmi che implementino un approccio di apprendimento federato eseguito in parallelo su una serie di UAV per migliorare la consapevolezza delle situazioni ambientali in uno scenario smart agriculture. Le tecniche di intelligenza artificiale edge saranno adottate a bordo degli UAV per elaborare dati raccolti dai sensori di vario tipo (ad es. sensori al suolo di posizione, temperatura, umidità, condizioni di irradiazione solare, e sensori di bordo e videocamere). Infine questa attività si occuperà della progettazione dell'interconnessione per la trasmissione dati tra droni e tra droni e terra e del sistema edge per la diffusione dei servizi intelligenti ondemand in base alle specifiche ETSI.

Titolo attività ricerca (ENG): "Mobile system for IoT data collection via drones and on-board processing"

Descrizione attività di ricerca (ENG): The main objective is to develop algorithms that implement a federated learning approach running in parallel on a series of UAVs to improve environmental situation awareness in a smart agriculture scenario. Edge artificial intelligence techniques will be adopted on board UAVs to process data collected by sensors of various types (e.g. ground sensors for position, temperature, humidity, solar radiation conditions, and on-board sensors and cameras). Finally, this activity will deal with the design of the interconnection for data transmission between drones and between drones and the ground and of the edge system for the dissemination of on-demand intelligent services based on ETSI specifications.

Responsabile scientifico: Prof. Giovanni Giambene

Sede prevalente di lavoro: Dpt. Ingegneria dell'Informazione e Scienze Matematiche - DIISM

Lingua straniera, livello di conoscenza richiesto: Inglese - Good

Modalità di svolgimento della prova: breve colloquio per verificare la conoscenza della lingua INGLESE al livello certificato dai titoli posseduti.

Indicazioni del progetto/programma di ricerca cui è collegato il contratto: Progetto "Supporting Project to Restart on Intelligent Networks for Telecommunications" (SPRINT) (cascade call PNRR del progetto NetwWin di RESTART – Spoke 8).

N. ore di didattica frontale: 15. L'attività didattica e di didattica integrativa e di servizio agli studenti sarà svolta nell'ambito degli insegnamenti afferenti al SSD di riferimento o a settori affini, che verranno previsti nel manifesto degli Studi a.a. 2024/2025 e successivi.

Numero massimo di pubblicazioni da presentare per la selezione (non inferiore a 12): 12

N. 1 posto – **Rif. 2**

Progetto: Bando a cascata Spoke 2 **-** FF4ALL - Detection of Deep Fake Media and Life-Long Media Authentication and related tasks

CUP: D43C22003050001

Dipartimento: Ingegneria dell'Informazione e Scienze Matematiche

Gruppo disciplinare: 09/IINF-03 Telecomunicazioni

Settore scientifico disciplinare: IINF-03/A Telecomunicazioni

Durata e tipo contratto: triennale/tempo pieno

Campo: Computer Science

Oggetto del contratto: Per ricercatore Junior: l'impegno annuo complessivo per lo svolgimento di attività didattica, di didattica integrativa e di servizio agli studenti è pari a 350 ore in regime di tempo pieno, e a 200 ore in regime di tempo definito.

Obiettivi di produttività: Svolgimento delle attività di ricerca collegate al progetto FF4ALL, compresa la produzione dei deliverable del progetto. Pubblicazione di articoli scientifici conseguenti all'attività del progetto. È prevista la pubblicazione di almeno 2 articoli all'anno (su rivista o in atti di convegno internazionale). Co-supervisione di eventuali dottorandi coinvolti nel progetto FF4ALL.

Per quanto concerne i diritti, i doveri e le modalità di svolgimento dell'attività si rinvia al Regolamento per i ricercatori a tempo determinato L. 240/2010 (D.R. 1891/2018).

Indicazioni del progetto/programma di ricerca cui è collegato il contratto: FF4ALL - Detection of Deep

Fake Media and Life-Long Media Authentication and related tasks

Titolo attività ricerca (ITA): Individuazione di immagini e video di tipo deepfake in ambiente ostile

Descrizione sintetica attività di ricerca (ITA): Lo sviluppo di strumenti forensi per il rilevamento di contenuti deepfake in un contesto avversariale inizierà con la definizione dei threat model, con la descrizione degli obiettivi e delle capacità esatte dell'analista forense e dell'attaccante. Sulla base dei modelli sviluppati, saranno ricercate soluzioni pratiche seguendo due approcci differenti: i) utilizzo di feature robuste e ii) addestramento avversariale. Nel primo caso, l'analisi si concentrerà sullo sviluppo di strumenti basati su feature semantiche, che, per loro natura, sono più resistenti ai tentativi di falsificazione dell'attaccante. Nel secondo caso, la sicurezza verrò ottenuta includendo campioni attaccati nel set di addestramento. A tal proposito, la ricerca si propone di studiare il compromesso tra accuratezza e robustezza nel caso specifico di modelli mirati a obiettivi forensi multimediali.

Titolo attività ricerca (ENG): Detection of Deepfake Images and Videos in Adversarial Setting

Descrizione attività di ricerca (ENG): The development of forensic tools for the detection of deepfake content in adversarial setting will start with the definition of the threat models describing the exact goals and capabilities of the forensic analyst and the attacker. Based on the threat models, practical solutions will be sought for by following two different approaches: i) use of robust features and ii) adversarial training. In the former case, the analysis will focus on the development of tools relying on sematic features, which, by their nature are likely to be more robust against falsification attempts made by the attacker. In the latter case, security against attacks is achieved by including attacked samples in the training set. On this regard, the research is expected to study the trade-off between accuracy and robustness in the specific case of models targeting multimedia forensic goals.

Responsabile scientifico: Prof. Mauro Barni

Sede prevalente di lavoro: Dipartimento di Ingegneria dell'Informazione e Scienze Matematiche - DIISM

Lingua straniera, livello di conoscenza richiesto: Inglese – Good

Modalità di svolgimento della prova: colloquio

N. ore di didattica frontale: 30 (annuali)

Numero massimo di pubblicazioni da presentare per la selezione (non inferiore a 12): 15

N. 1 posto – **Rif. 3**

Progetto: Bando a cascata Spoke 3 “Attacks and Defences”: Progetto AI-RESCUE

CUP: B63C24000490006

Dipartimento: Ingegneria dell’Informazione e Scienze Matematiche

Gruppo disciplinare: 09/IINF-03 Telecomunicazioni

Settore scientifico disciplinare: IINF-03/A Telecomunicazioni

Durata e tipo contratto: triennale/tempo pieno

Campo: Computer Science

Oggetto del contratto: l’impegno annuo complessivo per lo svolgimento di attività didattica, di didattica integrativa e di servizio agli studenti è pari a 350 ore in regime di tempo pieno, e a 200 ore in regime di tempo definito.

Obiettivi di produttività: Svolgimento delle attività di ricerca collegate al progetto AI-RESCUE, compresa la produzione dei deliverable del progetto. Pubblicazione di articoli scientifici conseguenti all’attività del progetto. È prevista la pubblicazione di almeno 2 articoli all’anno (su rivista o in atti di convegno internazionale). Co-supervisione di eventuali dottorandi coinvolti nel progetto. Per quanto concerne i diritti, i doveri e le modalità di svolgimento dell’attività si rinvia al Regolamento per i ricercatori a tempo determinato L. 240/2010 (D.R. 1891/2018).

Titolo attività ricerca (ITA): Applicazione di tecniche di adversarial machine learning alla rivelazione e attribuzione di immagini sintetiche in ambiente ostile

Descrizione sintetica attività di ricerca (ITA): Sviluppo di modelli teorici e strumenti pratici per l'applicazione di tecniche basate sull'intelligenza artificiale alla rilevazione e l'attribuzione di media sintetici in presenza di un avversario. L'analisi teorica e lo sviluppo di strumenti pratici verranno effettuati adottando due approcci complementari basati su diversi modelli di sicurezza: i) un'impostazione pessimistica di tipo white-box in cui si presume che l'attaccante abbia piena conoscenza delle tecniche utilizzate dall'analista, e ii) uno scenario più realistico in cui l'attaccante non ha o ha solo una conoscenza parziale degli strumenti (attacchi di tipo grey-box e black-box). In entrambi i casi, saranno presi in considerazione i punti di vista sia dell'attaccante che del difensore per determinare le prestazioni raggiungibili da entrambe le parti.

Titolo attività ricerca (ENG): Application of adversarial machine learning techniques to the detection and attribution of AI-synthetic images in the presence of adversaries

Descrizione attività di ricerca (ENG): Development of suitable theoretical models and practical tools for the application of AI-based techniques to the detection and attribution of synthetic media in the presence of an adversary. Both the theoretical analysis and the development of practical tools will be carried out by adopting two complementary approaches based on different security models: i) a pessimistic white-box setting wherein it is assumed that the attacker has full knowledge of the techniques used by the analyst, and ii) a more realistic scenario wherein the attacker has no or only partial knowledge about the tools (grey-box and black-box attacks). In both cases, the perspectives of both the attacker and the defender will be taken into account to determine the performance achievable by both parties.

Responsabile scientifico: Prof. Mauro Barni

Sede prevalente di lavoro: Dipartimento di Ingegneria dell'Informazione e Scienze Matematiche - DIISM

Lingua straniera, livello di conoscenza richiesto: Inglese - Good

Modalità di svolgimento della prova: colloquio

Numero massimo di pubblicazioni da presentare per la selezione (non inferiore a 12): 15