ICWMC 2024

The Tenth International Conference on Wireless and Mobile Communications

ISBN: 978-1-68558-131-2

March 10th –14th, 2024

Athens, Greece

ICWMC 2024 Editors

Jaime Lloret Mauri, Polytechnic University of Valencia, Spain

ICWMC 2024

Forward

The Twentieth International Conference on Wireless and Mobile Communications (ICWMC 2024), held between March 10th and March 14th, 2024, continued a series of international events on advanced wireless technologies, wireless networking, and wireless applications.

ICWMC 2024 addressed wireless related topics concerning integration of latest technological advances to realize mobile and ubiquitous service environments for advanced applications and services in wireless networks. Mobility and wireless, special services and lessons learnt from particular deployment complemented the traditional wireless topics.

We take here the opportunity to warmly thank all the members of the ICWMC 2024 technical program committee, as well as all the reviewers. The creation of such a high-quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and effort to contribute to ICWMC 2024. We truly believe that, thanks to all these efforts, the final conference program consisted of top-quality contributions. We also thank the members of the ICWMC 2024 organizing committee for their help in handling the logistics of this event.

We hope that ICWMC 2024 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress related to wireless and mobile communications.

ICWMC 2024 Chairs

ICWMC 2024 Steering Committee
Dragana Krstic, University of Niš, Serbia
Rajat Kumar Kochhar, Ericsson, Sweden
Magnus Jonsson, Halmstad University, Sweden
Sonia Ben Rejeb, Higher Institute of Computer Science (ISI), University of Tunis El Manar (UTM), Tunisia

ICWMC 2024 Publicity Chairs
José Miguel Jiménez, Universitat Politecnica de Valencia, Spain
Sandra Viciano Tudela, Universitat Politecnica de Valencia, Spain

ICWMC 2024
Committee

ICWMC 2024 Steering Committee

Dragana Krstic, University of Niš, Serbia
Rajat Kumar Kochhar, Ericsson, Sweden
Magnus Jonsson, Halmstad University, Sweden
Sonia Ben Rejeb, Higher Institute of Computer Science (ISI), University of Tunis El Manar (UTM), Tunisia

ICWMC 2024 Publicity Chairs

José Miguel Jiménez, Universitat Politecnica de Valencia, Spain
Sandra Viciano Tudela, Universitat Politecnica de Valencia, Spain

ICWMC 2024 Technical Program Committee

Mohamed Abid, University of Gabes, Tunisia
Bedoui Abla, CEDOC-2IT | INPT (National Institute of Posts and Telecommunication), Morocco
Afrand Agah, West Chester University of Pennsylvania, USA
Iness Ahriz, CNAM, France
Khalil Aissaoui, Tunisia Polytechnic School (TPS), Tunisia
Wafa Akkari, University of Manouba, Tunisia
Ali Kadhum M. Al-Quraby, University of Babylon, Iraq
Diego Alberto Godoy, Universidad Gastón Dachary, Argentina
Adel Aldalbahi, King Faisal University, Saudi Arabia
Adda Ali-Pacha, University of Sciences and Technology of Oran, Algeria
Karine Amis, IMT Atlantique, France
Tran Hai Anh, Hanoi University of Science and Technology (HUST), Vietnam
Antonio Arena, University of Pisa, Italy
Kamran Arshad, Ajman University, UAE
Nebojša Bačanin-Džakula, Singidunum University, Serbia
Salih Safa Bacanli, University of Central Florida, USA
Nedia Badri, ENSI - University of Manouba, Tunisia
Corey E. Baker, University of Kentucky, USA
Chaity Banerjee, University of Central Florida, USA
Kamel Barkaoui, Cedric | Cnam, France
Dimitri Belli, National Research Council (CNR) - Institute of Information Science and Technologies (ISTI), Pisa, Italy
Hadda Ben Elhadj, SM@RTS | Higher Institute of Informatics | Monastir University, Tunisia
Sonia Ben Rejeb, Higher Institute of Computer Science (ISI) - Higher School of Communications of Tunis (SUPCOM), Tunisia
Emna Ben Slimane, ENIT - Tunis El Manar University, Tunisia
Djamila Bendouda, Ecole Nationale Supérieur de Technologie, Algeria
Driss Benhaddou, University of Houston, USA
Djedjiga Benzid, École de Technologie Supérieure - Université du Québec, Canada
Vincent Beroulle, Grenoble INP, France

Robert Bestak, Czech Technical University in Prague, Czech Republic
Rui Bian, Expatiate Communications, USA
Petros S. Bithas, National and Kapodistrian University of Athens, Greece
Abdelmadjid Bouabdallah, University of Technology of Compiegne, France
Ridha Bouallegue, Higher School of Communications of Tunis "Sup'Com", Tunisia
Christos Bouras, University of Patras, Greece
Ines Bousnina, Tunisia Polytechnic School - University of Carthage, Tunisia
Brik Bouziane, Eurecom School, France
Maurizio Bozzi, University of Pavia, Italy
An Braeken, Vrije Universiteit Brussel, Belgium
Ibtissem Brahmi, University of Sfax, Tunisia
Marcos F. Caetano, University of Brasilia, Brazil
Jun Cai, Concordia University, Montreal, Canada
Rodrigo Campos Bortoletto, Federal Institute of Education, Science and Technology of São Paulo - IFSP, Brazil
Eric Castelli, CNRS / Laboratoire LIG, Grenoble, France
Nam Hoai Chu, University of Technology Sydney, Australia
Riccardo Colella, National Research Council of Italy, Italy
Nicolae Crisan, Technical University of Cluj-Napoca, Romania
Saber Dakhli, University of Carthage, Tunisia
Réjane Dalce, Institut de Recherche en Informatique de Toulouse (IRIT), France
Luca Davoli, University of Parma, Italy
Enrico Del Re, University of Florence and CNIT, Italy
Kapal Dev, Munster Technological University, Ireland
Sandesh Dhawaskar Sathyanarayana, University of Colorado Boulder, USA
Ding-Zhu Du, The University of Texas at Dallas, USA
Jalel Dziri, National Engineering School of Tunis, Tunisia
Eirini Eleni Tsiropoulou, University of New Mexico, USA
Ahmed EL-Sayed El-Mahdy, German University in Cairo, Egypt
Yaya Etiabi, Mohammed VI Polytechnic University, Benguerir, Morocco
Ahmed Fakhfakh, University of Sfax, Tunisia
Fairouz Fakhfakh, Universiy of Sfax, Tunisia
Faten Fakhfakh, National School of Engineering of Sfax, Tunisia
Przemyslaw Falkowski-Gilski, Gdansk University of Technology, Poland
Souhir Feki, University of Carthage, Tunisia
Miguel Franklin de Castro, Federal University of Ceará, Brazil
Mounir Frikha, Higher School of Communications of Tunis (SUPCOM), Tunisia
Marco Furini, University of Modena and Reggio Emilia, Italy
Jordi Garcia, CRAAX Lab - UPC BarcelonaTech, Spain
Krishna C. Garikipati, Niantic Inc., USA
Janusz Grzyb, Universityof Wuppertal, Germany
Abderrahmen Guermazi, Higher Institute of Technological Studies | National School of Engineers of Sfax | University of Sfax, Tunisia
Xiang Gui, Massey University, New Zealand
Habib Hamam, Université de Moncton, Canada
Abdelaziz Hamdi, ISITCOM | University of Sousse, Tunisia
Hicham Hammouchi, International University of Rabat (UIR), Rabat, Morocco
Wibowo Hardjawana, University of Sydney, Australia

Faisal Hussain, University of Engineering and Technology (UET), Lahore, Pakistan
Ali Kadhum Idrees, University of Babylon, Iraq
Muhammad Ikram, Macquarie University, Australia
Muhammad Ali Imran, University of Glasgow, UK
Faouzi Jaidi, University of Carthage, Higher School of Communications of Tunis & National School of Engineers of Carthage, Tunisia
Zakia Jellali, Higher School of Communication of Tunis (SUP'COM) | University of Carthage, Tunisia
Terje Jensen, Telenor, Norway
Wassim Jerbi, Higher Institute of Technological Studies | University of Sfax, Tunisia
Magnus Jonsson, Halmstad University, Sweden
Geethu Joseph, Syracuse University, USA
Georgios Kambourakis, University of the Aegean, Greece
Madhan Raj Kanagarathinam, Samsung R&D Institute, India
Lutful Karim, Seneca College of Applied Arts and Technology, Toronto / Moncton University, Canada
Eric Kerherve, Bordeaux INP, France
Wooseong Kim, Gachon University, S. Korea
Rajat Kochhar, Ericsson, Sweden
Peng-Yong Kong, Khalifa University, United Arab Emirates
Moez Krichen, Al Baha University, KSA / University of Sfax, Tunisia
Dragana Krstic, University of Niš, Serbia
Michel Kulhandjian, University of Ottawa, Canada
Vimal Kumar, University of *Waikato*, New Zealand
Souad Labghough, Mohammed V University in Rabat, Morocco
Mohamed Lamine Lamali, Univ. Bordeaux | LaBRI, France
Mohamed Latrach, ESEO / IETR - University of Rennes 1, France
SuKyoung Lee, Yonsei University, Seoul, South Korea
Ilhem Lengliz, Military Academy | HANALAB, Tunisia
Deyu Lin, Nanchang University, China
Eirini Liotou, National and Kapodistrian University of Athens, Greece
Jia Liu, Dalian University of Technology, China
Jian Liu, University of Tennessee, Knoxville, USA
Yueliang Liu, China University of Petroleum (East China), China
Maximilian Luebke, Friedrich-Alexander University Erlangen-Nürnberg, Germany
Sabri Lyazid, Université Bordj Bou Arreridj, Algeria / PARIS-UPEC, France
Stephane Maag, Institut Mines Telecom / Telecom SudParis, France
Setareh Maghsudi, University of Tübingen, Germany
Tianle Mai, Beijing University of Posts and Telecommunications, China
D. Manivannan, University of Kentucky, USA
Hend Marouane, Sfax University, Tunisia
Ahmed Mehaoua, University of Paris, France
Fanyi Meng, Tianjin University, China
Hamid Menouar, Qatar Mobility Innovations Center (QMIC), Qatar
Sofien Mhatli, ISI Kef | University of Jandouba, Tunisia
Fabien Mieyeville, University of Lyon | Université Claude Bernard Lyon 1 | CNRS, France
Farshad Miramirkhani, Isik University, Istanbul, Turkey
Jordi Mongay Batalla, Warsaw University of Technology, Poland
Raúl Montoliu Colás, Institute of new imaging technologies (INIT) - Jaume I University, Spain
Alireza Morsali, McGill University, Canada

Mohamed M. A. Moustafa, Egyptian Russian University, Egypt
Sami Myllymäki, University of Oulu, Finland
Assia Naja, International University of Rabat, Morocco
Sameh Najeh, Higher school of Communication (Sup'Com) of Tunis, Tunisia
Leïla Najjar, Higher School of Communication of Tunis (SUP'COM), Tunisia
Monia Najjar, University of Tunis El Manar, Tunisia
Leila Nasraoui, National School of Computer Sciences (ENSI) | University of Manouba, Tunisia
Nejah Nasri, National Engineering School of Sfax (ENIS_LETI_Tunisia), Tunisia
Idrissa Ndiaye, Université Cheikh Anta Diop, Senegal
Prasad Netalkar, Qualcomm, San Diego, USA
Armielle Ngaffo, Mediatron Laboratory, Tunisia
Maciej Nikodem, Wroclaw University of Science and Technology, Poland
Boubakr Nour, Beijing Institute of Technology, China
Diego Orlando Barragan Guerrero, Universidad Técnica Particular de Loja, Ecuador / ETS, Canada
Ekaterina Pakulova, Institute of Computer Science and Information Security of the Southern Federal University, Russia
Pablo Palacios, University of Chile, Chile
Tudor Palade, Technical University of Cluj-Napoca, Romania
Travis Peters, Montana State University, USA
Paulo Pinto, Universidade Nova de Lisboa, Portugal
Ivan Pires, Universidade da Beira Interior | Institute of Telecommunications, Portugal
Michele Polese, Institute for the Wireless Internet of Things | Northeastern University, USA
Valentin Radu, University of Sheffield, UK
Parisa Rafiee, George Washington University, USA
Adib Rastegarnia, Purdue University, USA
Heena Rathore, University of Texas, USA
Masood Ur Rehman, University of Glasgow, UK
Muhammad Atif Ur Rehman, Hongik University, South Korea
Éric Renault, ESIEE Paris, France
Francesca Righetti, University of Pisa, Italy
Miguel Rodríguez-Pérez, University of Vigo, Spain
Elisa Rojas, University of Alcala, Spain
Haidar Safa, American University of Beirut, Lebanon
Hajer Saidi, National Engineering School of Sfax, Tunisia
Varese Salvador Timóteo, Universidade Estadual de Campinas - UNICAMP, Brazil
David Sánchez-Rodríguez, University of Las Palmas de Gran Canaria, Spain
José Santa, Technical University of Cartagena, Spain
Adérito Seixas, Universidade Fernando Pessoa, Porto, Portugal
Oluyomi Simpson, University of Hertfordshire, UK
Soulayma Smirani, National Engineering School of Tunis (ENIT) | University of Tunis El Manar, Tunisia
Kaijun Song, University of Electronic Science and Technology of China, China
Marko Sonkki, Ericsson, Germany
Animesh Srivastava, Google, USA
Álvaro Suárez Sarmiento, Universidad de Las Palmas de Gran Canaria, Spain
Sheng Tan, Trinity University, USA
Fatma Tansu Hocanın, Cyprus International University, Lefkosa, TRNC
Rui Teng, Advanced Telecommunications Research Institute International, Japan
Hajer Tounsi, Ecole Supérieure des Communications de Tunis, Tunisia

Florian Tschorsch, TU Dresden, Germany
Sudhanshu Tyagi, Thapar Institute of Engineering & Technology | Deemed University, India
Rehmat Ullah, Hongik University, South Korea
Véronique Vèque, Université Paris-Saclay, France
Adrian Vidal, University of the Philippines Diliman, Philippines
Abdul Wahab, Queen Mary University of London, UK
Lei Wang, University of Connecticut, USA
Xianzhi Wang, University of Technology Sydney, Australia
You-Chiun Wang, National Sun Yat-sen University, Taiwan
Ulf Witkowski, South Westphalia University of Applied Sciences, Germany
Ouri Wolfson, University of Illinois at Chicago / University of Illinois at Urbana Champaign, USA
Diane Woodbridge, University of San Francisco, USA
Yuan Wu, University of Macau, Macau
Abid Yaqoob, Insight Centre for Data Analytics | Dublin City University, Ireland
Paul Yoo, University of London, UK
Sherali Zeadally, University of Kentucky, USA
Huanle Zhang, University of California, Davis, USA

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Enhancing Ultra-Wideband Localization Accuracy Using Spatial Filtering

Fahad Alsifiany
Department of IT and Artificial Intelligence
King Fahad Security College
Riyadh, Saudi Arabia
Email: sufyanyf@kfsc.edu.sa

***Abstract*—Ultra-Wideband (UWB) technology has emerged as a promising technology for use in precise indoor and outdoor localization systems, and has become handy for the rapidly growing fields of robotics and automation. The performance and accuracy of this technology are, however, affected significantly by multipath propagation, where the signals are exposed to reflection, scattering, and diffraction in the environment. This research embarks on improving UWB positioning accuracy by using spatial filtering techniques, with special emphasis on beamforming. A UWB localization model is developed for use in ranging for both indoor and outdoor environments. Theoretical modeling and simulations are then carried out to understand the influence of different environmental factors on the received UWB signals. Simulations are further carried out on the developed system, which utilizes beamforming to achieve spatial filtering of UWB signals. The experimental results show a significant improvement in UWB positioning accuracy compared to conventional non-beamforming methods.**

***Index Terms*—UWB; Spatial filtering; Beamforming; Accuracy; NLOS; LOS.**

I. INTRODUCTION

A. Localization Systems

Localization refers to the process of determining the exact or tentative location of an object, machine, or person in an indoor or outdoor environment. Most of the existing localization systems utilize technologies, such as Wi-Fi, Radio Frequency Identification (RFID), Infrared (IR), Global Positioning Systems (GPS), Bluetooth, and Ultra-Wideband (UWB). Most of the aforementioned technologies have been efficient for localization purposes in indoor environments. GPS particularly has been utilized in outdoor localization systems while UWB has proven to be efficient in both indoor and outdoor environments [1]. With the rapid growth of technology, there is a need for accurate localization systems. The fields of automation and robotics stand to benefit more from any forthcoming development in this field.

Despite being in existence for a long time, UWB technology has not been fully exploited [2]. This technology uses a broad spectrum of frequencies to transmit data over short distances with high data rates. The technology has proven to be more accurate in positioning as compared to other technologies [3]. Improving the accuracy of UWB localization would therefore offer us a futuristic solution to our growing localization needs.

B. Accuracy in UWB Systems

To improve accuracy, researchers have proposed different algorithms for use in UWB systems. They include advanced signal processing algorithms such as spatial filtering and Machine Learning (ML) algorithms [4] . In addition, optimized antenna arrays have been proposed to play an important role in achieving high spatial resolution and accuracy for these systems. By addressing the challenge of accuracy and implementing these strategies, UWB systems can realize their potential as reliable solutions for real-world applications [5].

C. Statement of the Problem

UWB technology is slowly gaining popularity as a promising technology to use for future localization needs. This is due to its ability to utilize a wide bandwidth, which gives it a high data rate capability. It also has low power consumption and has a better performance in Non-Line Of Sight (NLOS) scenarios and cluttered spaces than other localization technologies. This also makes it suitable for use in both indoor and outdoor environments. The accuracy of UWB localization systems is critical for their successful deployment in its various applications. This research explores a conventional beamforming algorithm as a spatial filtering technique to suppress unwanted signals due to multipath and interference, to realize accurate localization of objects using UWB technology.

D. Aims and Objectives

i. Develop a spatial filtering technique for use in UWB systems to improve the accuracy of localization in both indoor and outdoor environments.
ii. Implement a conventional beamforming algorithm to enhance UWB signal directionality and mitigate interference and multipath effects.
iii. Test the developed model through real-world experiments and simulations, comparing its performance with existing accuracy-improvement methods for UWB localization systems.

The rest of this paper is organized as follows. Section II introduces the related work. Section III presents the theoretical framework. Section IV describes the methodology approach. In Section V, results and discussion are shown. Finally, conclusions are drawn in Section VI.

II. RELATED WORK

Multiple researches have been conducted with an aim of improving the accuracy of UWB localization. The authors in [1] propose a UWB localization system utilizing Adaptive Kalman Filter to improve its accuracy. This realized improvement accuracy by significantly reducing the noise in measurements and NLOS effects. This work is similar to [4], which proposes an efficient Iterated Adaptive Kalman Filter (IAKF) algorithm for indoor positioning drift correction. The research contributes to addressing one of the major challenges in UWB localization, which is the accumulation of errors over time. The IAKF method demonstrates promising results in minimizing drift, thus improving the accuracy of UWB-based systems.

The authors in [2] investigate UWB positioning accuracy in a warehouse environment. Their research addresses the challenges posed by complex indoor settings, such as multipath effects and non-line-of-sight UWB signal propagation. In [3], an indoor positioning system utilizing UWB technology based on a digital twin concept is presented. This work explores the potential of integrating virtual models of the physical environment to enhance UWB-based positioning accuracy. The digital twin approach allows for real-time adjustments and optimizations, thereby improving the overall accuracy and reliability of the system.

The authors in [6] develop an UWB indoor positioning algorithm under the influence of human occlusion and spatial non-line-of-sight conditions. This study acknowledges the impact of human presence on UWB signal propagation. The work also investigates techniques to mitigate localization errors caused by these factors. This work proposes the development of robust algorithms for improving the accuracy of UWB systems in dynamic real-world scenarios.

In [7], the authors contribute to this field by outlining key algorithms that would go a long way to improve the ranging in UWB systems. These algorithms include Unilateral Dual Range Ranging, Symmetrical Two-Way Round Range Ranging (SDS-TWR) and Asymmetric Bilateral Two-Way Ranging (ADS-TWR).

The authors in [8] introduce an Indoor Positioning System (IPS) utilizing UWB technology for the Industrial Internet of Things (IIoT). The study supports the use of UWB-based localization in industrial applications. It also highlights the potential impact of accurate indoor positioning on IIoT systems.

In [9], deeper insights into UWB-based indoor localization techniques are provided. This serves as a foundation for the broader exploration of advanced spatial filtering approaches, such as beamforming presented in this work.

III. THEORETICAL FRAMEWORK

A. UWB Technology

UWB devices operate at a frequency between 3.1 GHz and 10.6 GHz. UWB technology offers several advantages, including immunity to multi-path losses and the ability to transmit signals through opaque media. It can also be delivered over wire cables, providing increased bandwidth without requiring changes to existing infrastructure. UWB devices can operate at very low power, allowing for multiple users and a data rate exceeding 100 Mb/s. Additionally, UWB signals are difficult to detect due to their wide bandwidth, and communication can be done securely through unique randomization of codes at a million bits/s. UWB technology provides robust communication due to its large processing power.

B. Line Of Sight (LOS) and Non-Line Of Sight (NLOS) Propagation of UWB Signals

Line-Of-Sight (LOS) propagation of UWB signals occurs when the signal travels in a straight line between a transmitter and receiver without any significant obstructions. This results in low attenuation, high Signal-to-Noise Ratio (SNR), and minimal delay spread, making it ideal for high accuracy applications such as radar imaging, location tracking, and wireless communication. However, in real-world environments, obstacles such as buildings, trees, and walls can cause signal blockage, reflection, diffraction, and scattering, leading to NLOS propagation that can significantly affect the performance and reliability of UWB systems. To mitigate these effects, techniques such as adaptive antenna arrays, time-of-arrival estimation, and angle-of-arrival estimation can be used to improve signal quality and reduce errors in UWB communication systems.

Figure 1 shows UWB signals propagation in LOS and NLOS scenarios [10].

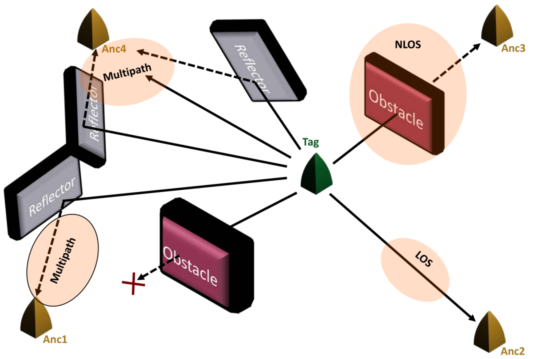


Figure 1. LOS and NLOS propagation of UWB signals [10].

C. UWB Localization Systems

UWB localization systems utilize different algorithms for measurement approximations. These algorithms include:

- Time Of Arrival (TOA)
- Angle Of Arrival (AOA)
- Received Signal Strength (RSS)
- Time Difference Of Arrival (TDOA)
- Hybrid algorithms

1) AOA based algorithms: In these algorithms, two sources are considered in estimating the angle at which a signal is received at the receiver end. The angle of signal reception is then compared to the carrier phase across different antennas or the amplitude of the signal. The intersection of the angle line for each source of the signal is taken to be the location. This algorithm is complex and the geometry of the antenna array determines its accuracy. Figure 2 illustrates the AOA based algorithm [10].

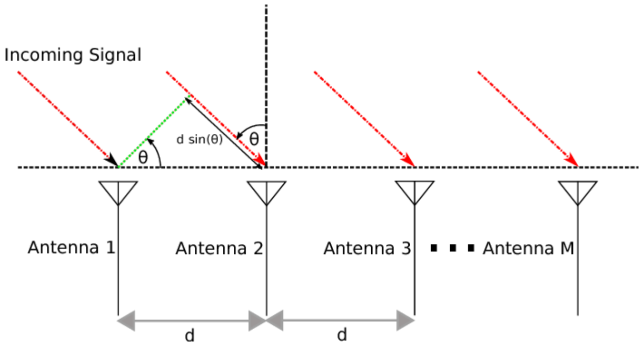


Figure 2. Angle Of Arrival (AOA) [10].

2) TOA based algorithms: These algorithms assume arbitrary circles around multiple transmitters. The radius of these circles is taken to be the distance between the transmitter and receiver. The intersection of these circles is the point of interest [4]. Time synchronization is necessary for the transmitters but not as important for the receivers. The one-way propagation time between the transmitter and receiver helps in calculating the distance between them. Any observable delay needs to be accounted for in the calculation.

3) TDOA based algorithms: These algorithms rely on calculating the time difference in the arrival of a signal sent by one transmitter and received by three or more receivers. A single receiver would also be used to estimate the delta variations in the arrival times of two transmitted signals [5]. These algorithms require significant bandwidth as typically in UWB positioning, only one transmitter is available, which means that all receivers have to work in synchrony to determine the time delay in the arrival of the transmitted signal. Figure 3 is an illustration of a TDOA-based algorithm [11].

4) RSS based algorithms: The target being tracked monitors the signal strengths of signals from different transmitters and uses them to estimate the distance between these transmitters and receivers. This allows the receiver to calculate its relative position with respect to the transmitting nodes. These algorithms are however unpopular as they have poor accuracy in NLOS signal propagation and in multipath environments.

5) Hybrid algorithms: Depending on the environment where an adaptive positioning system needs to be deployed, hybrid algorithms can be used. These algorithms combine the efficiencies of two or more of the aforementioned algorithms to increase the accuracy of ranging. This approach, however, increases the expense and complexity of the system equally.

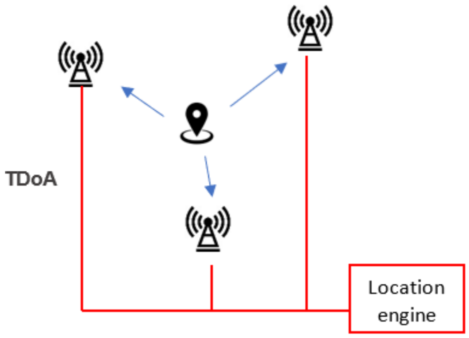


Figure 3. Time Difference Of Arrival (TDOA) [11].

IV. METHODOLOGY

The Qorvo DWM1000 IC Modules were used as the UWB transceiver modules. This UWB module allows items to be located in Real-Time Location Systems (RTLS) with a resolution of up to 200 meters. It is also compatible with a wide range of micro-controller units (MCUs). The frequency range of this transceiver module is 3.5 GHz to 6.5 GHz. Figure 4 shows the Qorvo DWM1000 IC Module.

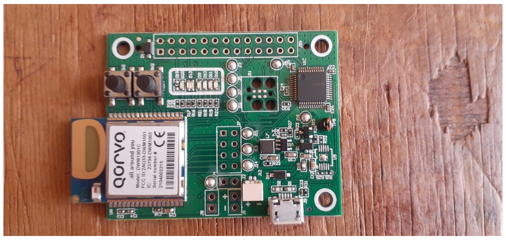


Figure 4. Qorvo (DWM1000) IC Module.

In the first set-up, a Qorvo DWM1000 module was defined as the anchor transceiver. Another transceiver was placed at a distance of 30m as the tag transceiver. Localization was then performed on the tag transceiver from the anchor, and the ranged distances recorded against each of the actual distances. The tag transceiver was further moved to distances of 90 and 160m. This was carried out in two different environments. In one environment, an indoor space with cluttered space was used. The UWB signal was forced to navigate through walls and around obstacles to understand UWB performance when subjected to multipath effects. In the other environment, an outdoor space was chosen, with no obstacles and with a clear LOS. In the second set-up, 5 UWB transceivers were used as the tags. These transceivers were placed at similar distances as for those of the first set-up. Localization was then done, and the ranged distances recorded against the actual distances. This was carried out for both an indoor cluttered space and an outdoor environment.

The accuracy for the developed system was then evaluated as a percentage using the ranged and the actual distances, and

ISBN: 978-1-68558-131-2

the corresponding SNR recorded. The behavior of this system was then modeled on MATLAB software. A conventional beamforming algorithm was then developed. The beamforming algorithm was used to perform spatial filtering on the modeled UWB signal, as derived from its real-world behavior.

The modeled conventional beamforming algorithm is detailed below.

Let $x(t)$ be the UWB signal of interest, and $n(t)$ be the additive noise. The received signal at antenna i can be expressed as:

$$y_i(t) = h_i \cdot x(t - \tau_i) + n_i(t), \tag{1}$$

where $y_i(t)$ is the received signal at antenna i at time t, h_i represents the channel gain of antenna i, τ_i is the time delay of signal arrival at antenna i, and $n_i(t)$ is the noise at antenna i.

Calculate the beamforming weights $\mathbf{w}_i$ for each antenna element i to focus the reception towards the desired direction of arrival:

$$\mathbf{w}_i = \frac{1}{N} e^{j \cdot 2\pi f_c \tau_i}, \tag{2}$$

where f_c is the carrier frequency.

The beamformed signal $\mathbf{s}(t)$ can be obtained by combining the received signals from all antennas after applying the beamforming weights:

$$\mathbf{s}(t) = \sum_{i=1}^{N} w_i \cdot \mathbf{y}_i(t). \tag{3}$$

Assuming the use of Time Of Arrival (ToA) method for localization, one can estimate the time delay τ from the received beamformed signal $\mathbf{s}(t)$ and use it to calculate the distance d to the source:

$$\tau = \arg\max_t |\mathbf{s}(t)|, \tag{4}$$

$$d = \frac{c \cdot \tau}{2}, \tag{5}$$

where c is the speed of light.

Algorithm 1 Beamforming Algorithm

```
UWB signal measurements from $N$ antennas.
for $i = 1$ to $N$ do
    Compute $\tau_i$ (time delay).
    Compute $w_i = \frac{1}{N} e^{j \cdot 2\pi f_c \tau_i}$ (Beamforming weight).
end for
Beamformed signal $s(t) = 0$.
for $i = 1$ to $N$ do
    Obtain received signal $y_i(t)$ from antenna $i$.
    Weighted signal contribution: $s(t) \mathrel{+}= w_i \cdot y_i(t)$.
end for
Estimate time delay $\tau = \arg\max_t |s(t)|$.
Compute distance to source: $d = \frac{c \cdot \tau}{2}$.
```

V. RESULTS AND DISCUSSION

The modeled UWB system exhibited minimal variations of results for localization conducted in indoor and outdoor environments. This shows the efficiency of UWB signals to offer accurate localization even in cluttered indoor spaces.

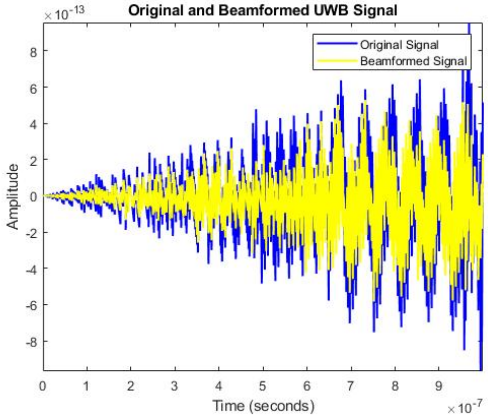


Figure 5. Localization at 30m using 2 antennas.

Figure 5 displays a plot of the pulses for the original UWB signal and the beamformed UWB signal for a localization distance of 30m between 2 antennas in an indoor environment. The plot indicates a reduction in amplitude in the beamformed signal compared to the original signal.

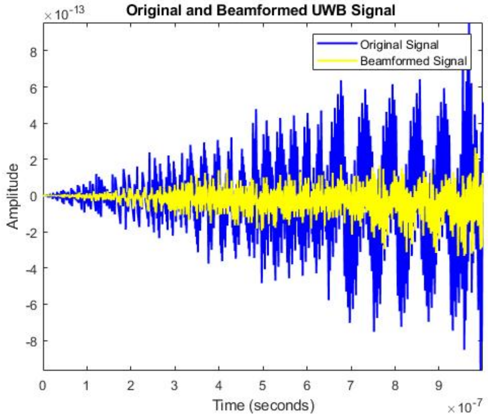


Figure 6. Localization at 30m using 6 antennas.

Figure 6 presents a plot of the pulses for the original UWB signal and the beamformed UWB signal for a localization distance of 30m between 6 antennas in an indoor setting. There is a significant decline in amplitude in the beamformed signal relative to the original signal.

Figure 7 shows a plot of the pulses for the original UWB signal and the beamformed UWB signal for a localization distance of 160m between 2 antennas in an indoor environment. The plot indicates a reduction in amplitude in the beamformed signal compared to the original one.

Figure 8 illustrates a plot of the pulses for the original UWB signal and the beamformed UWB signal for a localization dis-

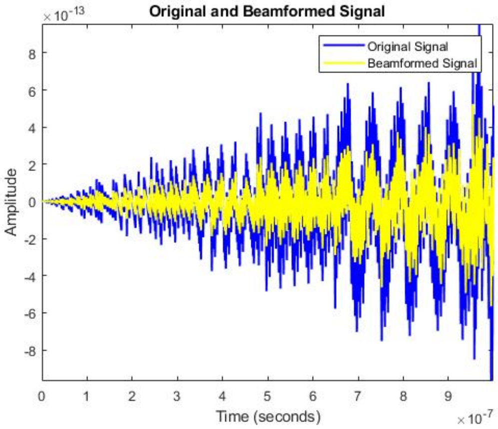


Figure 7. Localization at 160m using 2 antennas.

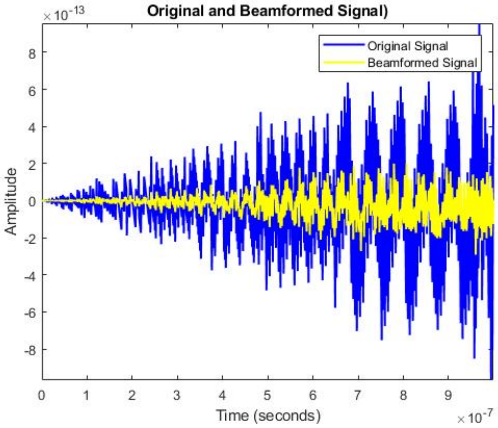


Figure 8. Localization at 160m using 6 antennas.

tance of 160m between 6 antennas in an indoor environment. The plot demonstrates a significant reduction in amplitude in the beamformed signal relative to the original signal.

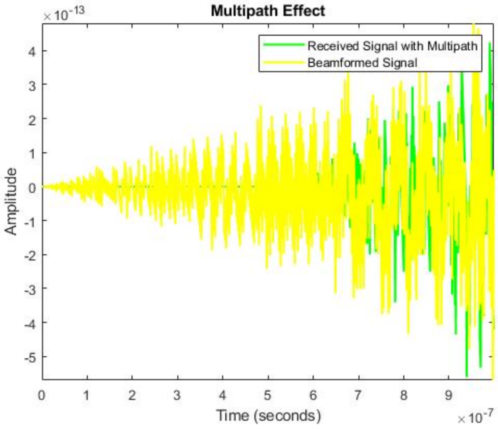


Figure 9. Multipath effect using 2 antennas.

Figure 9 demonstrates the impact of conventional beamforming on a signal under NLOS propagation with multipath effects during localization using 2 antennas.

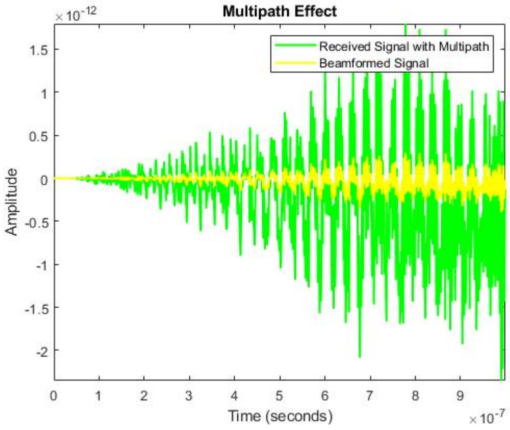


Figure 10. Multipath effect using 6 antennas.

Figure 10 shows the effect of conventional beamforming on a signal in a Non-Line-of- Sight (NLOS) propagation with multipath effects while performing localization using 6 antennas.

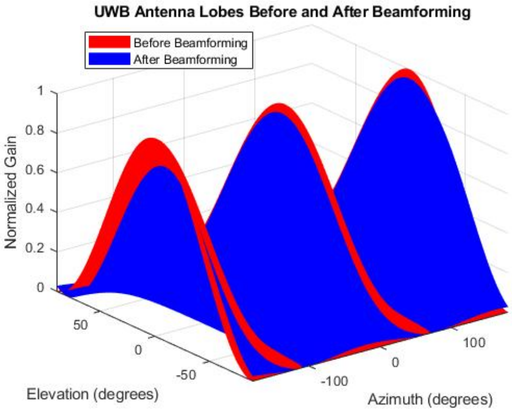


Figure 11. Beamformed and Non-Beamformed lobes.

Figure 11 depicts the signal lobes of the original and beamformed UWB signal in a modeled system that uses 4 antennas for localization, whereby one antenna serves as the anchor while the rest serve as the tags, in an indoor environment.

Figure 12 is a depiction of the accuracy prior to and post-beamforming. The maximum realized ground-truth accuracy for the developed system was around 99.5% while the maximum accuracy realized after beamforming reached 100%.

There was a significant reduction in the amplitude of the beamformed signals compared to the original signals. This property is associated with beamforming, where energy is directed in a particular direction, resulting in lower amplitudes in other directions. However, this does not necessarily represent the efficiency of the developed conventional beamforming algorithm.

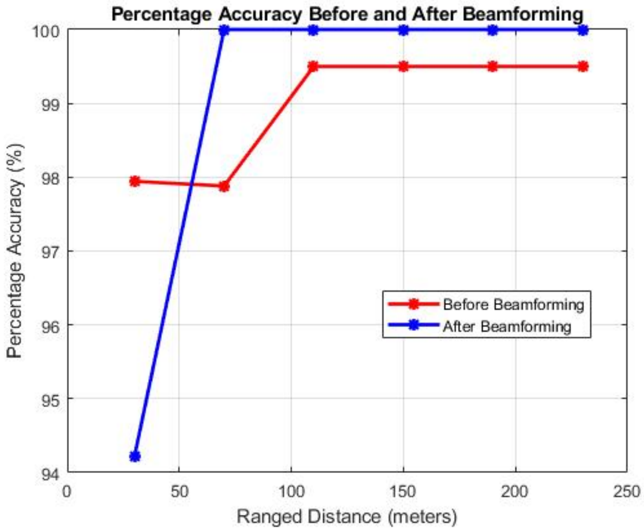


Figure 12. Beamformed and Non-Beamformed accuracy.

In an attempt to establish the accuracy of the system, the SNR metric was used. By analyzing the change in SNR before and after beamforming, there was a significant measure of improvement in signal quality, which in turn played an essential role in enhancing local accuracy.

Beamforming proved more effective at longer distances than at shorter distances. This was particularly observed using multiple antennas, which notably contributes to signal diversity in the received signals. UWB signals ranged at long distances increase multipath attenuation, which can lead to signal degradation. However, the use of several antennas take advantage of the different signal properties to produce a signal with improved localization accuracy. This further supports the high efficiency levels observed in UWB localization for NLOS propagation, where optimal results were realized while utilizing multiple antennas.

VI. CONCLUSION AND FUTURE WORK

Through empirical experimentation and MATLAB simulations, the study confirmed that beamforming significantly enhances UWB-based localization accuracy. Despite the noticeable reduction in beamformed signal amplitude, a result of focused power, the SNR emerged as a strong indicator of improved accuracy. Furthermore, the study revealed that leveraging multiple antennas further improved beamforming accuracy due to signal diversity. This was particularly effective in mitigating multipath fading and enhancing the performance of UWB in NLOS environments.

One of the limitations of the developed algorithm was its over-reliance on signal diversity provided by multiple antennas. There was notably low accuracy while using fewer antennas. This would translate to an increased implementation cost for the proposed system. Another limitation of the developed system is that accuracy relied on the Signal-to-Noise Ratio (SNR) as the key metric, potentially overlooking important aspects of performance such as robustness to interference.

Future research will focus on combining conventional beamforming algorithms with advanced beamforming algorithms such as ML systems to further improve the accuracy in UWB localization systems. This would stand to make UWB-based localization robust for our future localization needs and further strengthen its application in real-world scenarios.

ACKNOWLEDGMENT

I would like to express my gratitude to the General Director of King Fahd Security College (KFSC), Major General Dr. Ali Al-Duaij, for his support in this project.

REFERENCES

[1] C. Yi, A. Z. Da, C. Hui, C. Shan, and Z. Xuan, “A UWB location algorithm-Based on adaptive Kalman filter,” in *Journal of Physics: Conference Series*, vol. 1757, no. 1. IOP Publishing, 2021, p. 012176.
[2] Z. Wang, S. Li, Z. Zhang, F. Lv, and Y. Hou, “Research on UWB positioning accuracy in warehouse environment,” *Procedia computer science*, vol. 131, pp. 946–951, 2018.
[3] P. Lou, Q. Zhao, X. Zhang, D. Li, and J. Hu, “Indoor positioning system with UWB based on a digital twin,” *Sensors*, vol. 22, no. 16, p. 5936, 2022.
[4] S.-H. Lin, H.-H. Chang Chien, W.-W. Wang, K.-H. Lin, and G.-J. Li, “An Efficient IAKF Approach for Indoor Positioning Drift Correction,” *Sensors*, vol. 22, no. 15, p. 5697, 2022.
[5] C. L. Sang, B. Steinhagen, J. D. Homburg, M. Adams, M. Hesse, and U. Rückert, “Identification of NLOS and multi-path conditions in UWB localization using machine learning methods,” *Applied Sciences*, vol. 10, no. 11, p. 3980, 2020.
[6] H. Zhang, Q. Wang, C. Yan, J. Xu, and B. Zhang, “Research on UWB Indoor Positioning Algorithm under the Influence of Human Occlusion and Spatial NLOS,” *Remote Sensing*, vol. 14, no. 24, p. 6338, 2022.
[7] Y. Liu, “Research on indoor positioning algorithms based on ultra-wideband technology,” in *International Conference on Computer, Artificial Intelligence, and Control Engineering (CAICE 2023)*, vol. 12645. SPIE, 2023, pp. 1070–1076.
[8] F. Che, Q. Z. Ahmed, P. I. Lazaridis, P. Sureephong, and T. Alade, “Indoor Positioning System (IPS) Using Ultra-Wide Bandwidth (UWB)—For Industrial Internet of Things (IIoT),” *Sensors*, vol. 23, no. 12, p. 5710, 2023.
[9] S. Mohanty, A. Tripathy, and B. Das, “UWB Based Indoor Localization Techniques,” *Technology*, vol. 5, p. 6, 2003.
[10] M. Schüssel, “Angle of arrival estimation using WiFi and smartphones,” in *Proceedings of the International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, vol. 4, 2016, p. 7.
[11] U. Hany *et al.*, “Accuracy of UWB Path Loss-Based Localization of Wireless Capsule Endoscopy,” *Journal of Healthcare Engineering*, vol. 2023, 2023.

Collusion Resistant Watermarking Using Convolutional Encoding and Random Spreading

Abdul Rehman
IRT b-com
Cesson-Sevigné, France
abdul.rehman@b-com.com

Gaëtan Le Guelvouit
IRT b-com
Cesson-Sevigné, France
gaetan.leguelvouit@b-com.com

Jean Dion
IRT b-com
Cesson-Sevigné, France
jean.dion@b-com.com

Frédéric Guilloud
IMT Atlantique, Lab-STICC
Brest, France
frederic.guilloud@imt-atlantique.fr

Matthieu Arzel
IMT Atlantique, Lab-STICC
Brest, France
matthieu.arzel@imt-atlantique.fr

***Abstract*—This paper presents a Discrete Wavelet Transform based collusion resistant video watermarking to trace colluders involved in unauthorized video distribution. Our scheme uses Tardos-Skoric codes as fingerprints. To reduce the errors on the fingerprinting codes, we propose a joint scheme that combines pseudo-random spreading sequences and convolutional codes. The performance when the fingerprint embedding and the attack are simulated as a binary symmetric channel proves that the proposed scheme performs better in terms of bit error rate and in terms of colluders tracing using binary attacks. Simulations of a darken attack on the watermarked videos show promising results for low to moderate opacities of the fingerprint embedding.**

Keywords*—*Video watermarking; collusion; fingerprinting codes; convolutional encoding; spreading.

I. INTRODUCTION

In the age of wide digital content distribution, it is now more crucial than ever to provide reliable and powerful techniques to prevent unauthorized redistribution of multimedia objects [1] [2] denoted as collusion attacks. In collusion attacks, multiple users merge their content to alter the watermark, making it difficult to trace these users who are the source of unauthorized copies and thus posing a significant threat to traditional watermarking methods [3] [4]. Tardos codes, proposed in 2003 by Tardos [5], are collusion-resistant codes which were the first theoretically proven codes to efficiently prevent illegal redistribution of digital content. The principle of collusion-resistant watermarking is to associate a unique fingerprint per subscriber into each copy of the content. After the collusion attack, Tardos codes enable the content distributor to retrieve the subscribers responsible for the creation and redistribution of the illegal content. The length of Tardos codes is given by [5] as $100{c_0}^2 \ln \frac{1}{\varepsilon_1}$ and depends on the number of colluders to trace, c_0, and on the probability of accusing any innocent user, ε_1. Tracing more colluders implies higher fingerprinting lengths and brings more difficulties to hide the fingerprint into the video. Later on, Skoric et al. [6] reduced the Tardos code length approximatelt 5 times taking into account the number of users n, coming up with a length $\frac{1}{2}\pi^2 {c_0}^2 \ln \frac{n}{\varepsilon_1}$. In this study, we use Skoric codes as fingerprinting codes against collusion attacks.

The problem is that embedding fingerprints into videos adds noise yielding binary errors on the fingerprint, and consequently decreasing the performance of Tardos-Skoric codes. This is the reason why numerous studies take advantage of pseudo-random spreading [7]–[11] to hide data into images with low errors after retrieving the data. In a recent study [14], we also used random spreading to hide Tardos-Skoric generated fingerprints in a watermark image and found out the best generator-decoder combination of collusion codes for real time implementation to find at-least one colluder. However, the gain provided by random spreading is decreased as the fingerprint length is increased for a given image size. To improve the performance of random spreading, we propose to use Error Correcting Codes (ECC).

The authors in [12] demonstrated that using convolutional encoding with Discrete Wavelet Transform (DWT) watermarking provided enhanced resistance to multimedia compression, but without addressing other crucial attacks, such as collusion, geometric distortions and cropping. In [13], the authors illustrate the robustness of a watermarking scheme for images using convolutional codes embedding, and considering all standard multimedia attacks. However, collusion attacks are not adressed. Also, watermarking in this study is non-blind, meaning that the original image is required. In this article, we focus on blind watermarking: the original content is not available at the receiver side. Convolutional encoding and random spreading are also combined in [15] to lower the bit error rate brought on by interference from the host signal. However, in the simulations, no attacks of any kind were taken into account. In this work, we propose to use convolutional codes either concatenated with random spreading or jointly, as proposed in [15], to improve colluders tracing in collusion attacks.

Our paper is organized as follows. In Section II, we review the fundamentals of watermarking and illustrate the need for spreading when using collusion codes. Then, we describe the two proposed spreading schemes using convolutional codes: a joint scheme and a concatenated spreading schemes. The performance of these spreading schemes is presented in Sec-

ISBN: 978-1-68558-131-2

tion III, first over a binary symmetric channel, and then for collusion tracing in a realistic scenario where the fingerprint is embedded into the videos and where a real collusion attack is performed. Conclusions and perspectives are presented in Section IV.

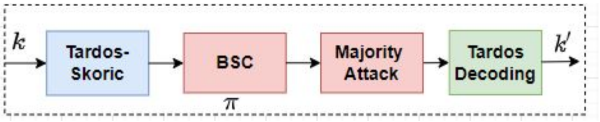
II. COMBINING CODING AND SPREADING FOR WATERMARKING

A. Motivation

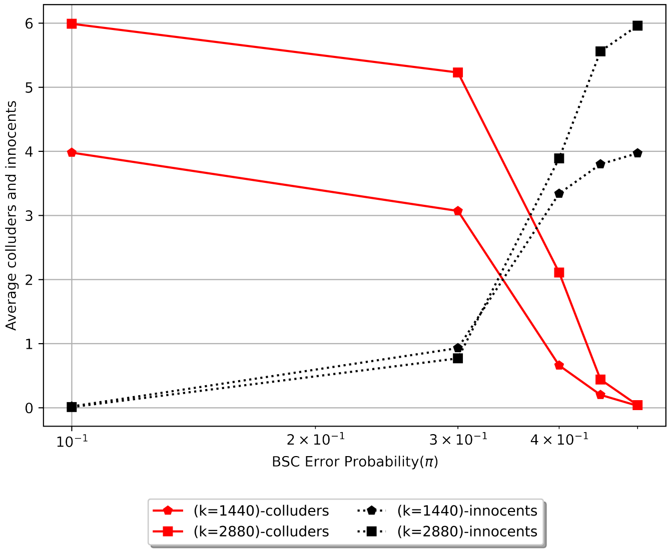
1) Definition and Notations: In collusion resistant video watermarking, a Tardos-Skoric fingerprinting code of length k is hidden into an image to trace the colluders. To trace a higher number of colluders among many users requires higher k. The maximum value of k to be hidden in a $360p$ image corresponds to the image size given by 360×640. The watermarked image I_{wt} is obtained by alpha blending $I_{wt} = \mathscr{O} I_i + (1-\mathscr{O}) I_w$, where $\mathscr{O}$ is the opacity ranging between 0 and 1, I_w is the watermark image (the information to be hidden, e.g., the fingerprint code) and I_i is the original image. We employed DWT with level-3 to obtain I_w from the fingerprint. Note that we omit the LL3 (lowest frequency) part of the DWT since it cannot be reproduced in a blind detection of the watermark image [16]. We thus come up with the final watermark image size $m = (360 \times 640) - LL3 = 226800$ corresponding to the maximum value for the fingerprint code k. However, watermarking should be discrete. To accomplish this, the opacity $\mathscr{O}$ has to be very close to 1 yielding a power ratio between the watermark image I_w and the watermarked image I_{wt} to be as low as about -20dB, depending on the considered image.

2) Impact of binary errors on the Tardos-Skoric codes: For such low SNRs, many errors occur in the fingerprint, which leads to dramatic performance for collusion tracing with Tardos-Skoric codes. We analyzed the performance of Tardos-Skoric codes using the majority vote attack to trace out the colluders without any spreading. The simulation model is depicted in Figure 1(a): Tardos-Skoric codes are modified by a Binary Symetric Channel (BSC) with error probability π, which represents the possible errors due to the embedding with a low Signal over Noise Ratio (SNR). Figure 1(b) illustrates that, whatever the length of the fingerprint k, the number of average detected colluders drops for binary error probabilities higher than $\pi = 2 \times 10^{-1}$, which corresponds to a much higher SNR than -20dB.

A well known way to improve SNR is to spread the fingerprint length k over the image length m. Let α denote the spreading rate $\alpha = \frac{k}{m}$. A lower α results in fewer binary errors on the watermark image but, but as the image length is fixed, it also resultsin lower fingerprint k, reducing total colluders detecting capacity. In this Section, firstly, we propose to improve the efficiency of the spreading by combining pseudo-random sequences with ECC. Then, we address the issue of optimizing the spreading rate α for a fixed image length m.



(a) Simulation model



(b) Simulation results

Figure 1: Colluders tracing without spreading scheme for majority vote attack: (a) Simulation model (b) Average detected colluders with $k = [1440, 2880], n = 1000$ and $\varepsilon_1 = 10^{-3}$.

B. Proposed Spreading Schemes

1) Convolutional Codes and Viterbi Decoding: Although convolutional codes have been surpassed by many others, they are still often used in watermarking. The authors from [17]–[19] showed that using convolutional codes with fragile watermarking improves the SNR but also that the scheme is not robust to compression, contrast enhancement and collusion attacks. In this paper, we propose to use convolutional codes to increase the robustness against noise on embedded collusion codes. A convolutional code [20] is specified by its coding rate r_{cc} and the depth N of its shift register. The trellis diagram is a result of expanding the convolutional code state diagram in time. The number of the states in the trellis diagram is 2^N. To decode a convolutional code, we generally use the Viterbi algorithm [20], which finds efficiently the shortest path on the trellis diagram.

2) Combination of coding and pseudo-random sequences: Two spreading schemes using convolutional codes are proposed hereafter: the concatenated scheme and the joint scheme.

For the concatenated scheme, the convolutional encoder is utilized to encode the k bits of the fingerprint with rate r_{cc}. The trellis shown in Figure 2(a) illustrates the outputs of the convolutional encoder of rate $r_{cc} = 1/2$ with $N = 2$ for each possible transition between 2 states. The output of the encoder is then spread using pseudo-random sequences of rate $\frac{\alpha}{r_{cc}}$.

In the joint scheme, the k bits of fingerprint are encoded and spread simultaneously utilizing joint convolutional encoding and spreading with rate α, as proposed by [15]. In this scheme, the outputs are given pseudo-random sequences s_{r_i} with $i \in [1,\ldots,2\times 2^N]$ of rate $\frac{1}{\alpha}$, as illustrated in Figure 2(b).

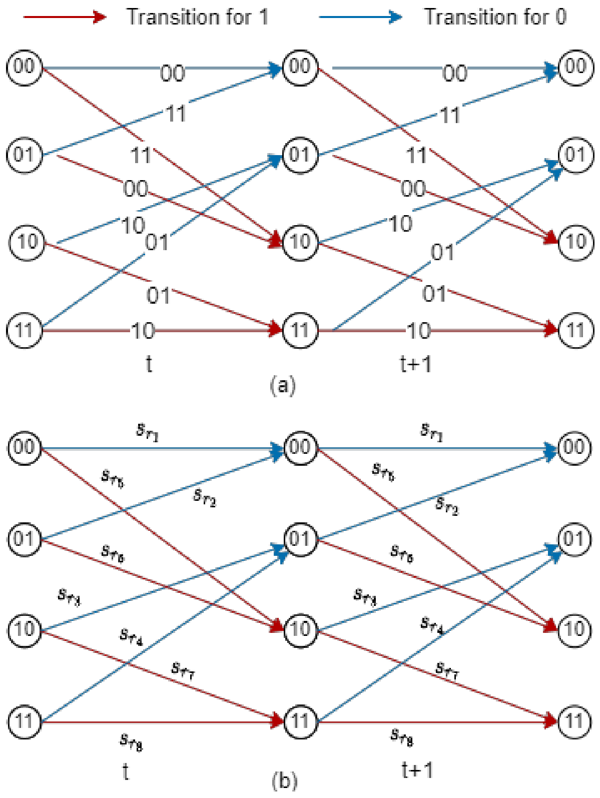


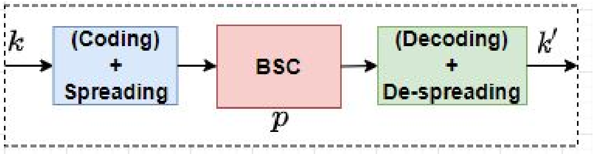
Figure 2: Trellis diagram for 4 states: (a) concatenated scheme with rate $r_{cc} = \frac{1}{2}$ (b) joint scheme with rate $\frac{1}{\alpha}$.

C. Performance comparison

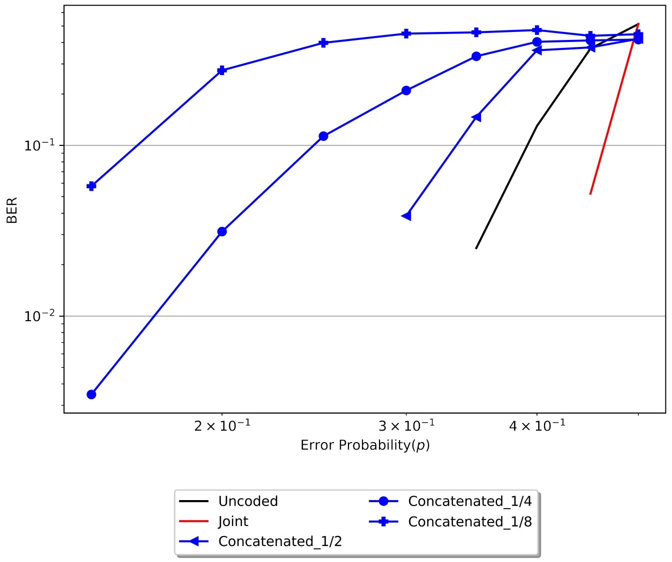
We evaluated the performance of the spreading using a Binary Symmetric Channel (BSC) with error probability p, as shown in Figure 3(a). For performance evaluation, the concatenated and joint schemes are compared with a pure pseudo-random spreading scheme denoted ”uncoded” since no convolution code is used.

For the concatenated scheme, we compare three different numbers of shift register: $N = 3,5$ and 9, respectively, associated with 3 different rates $r_{cc} = \frac{1}{2}, \frac{1}{4}$ and $\frac{1}{8}$. The random spreading rates after encoding are thus, respectively, $2\alpha, 4\alpha$ and 8α. Simulations have been performed for $\alpha = 1/157$ (k being set to 1440) and are illustrated in Figure 3(b). The joint scheme clearly outperforms the two other schemes. Note, however, that the uncoded scheme outperforms the concatenated scheme, thus showing that convolutional codes not always improve the spreading performance.

To determine a viable fingerprint length with an acceptable BER, we investigated the trade-off between spreading rate and BER. We performed simulations considering different fingerprint lengths $k = [256, 512, 1024, 1440, 2880]$. Considering the BER target of 2.10^{-1}, the selected possible fingerprint lengths are $k = 2880$ for the joint scheme and $k = 1440$ for the uncoded scheme, as shown in Figure 4. These trade-offs correspond to a spreading rate of $alpha = [1/157, 4/315]$, respectively, for lengths $k = [1440, 2880]$.



(a) Simulation model



(b) Simulation results

Figure 3: Bit Error Rate (BER) for spreading schemes combined with convolutional codes and compared to a pure random spreading scheme (uncoded) BSC with error probabilities p for a spreading rate $alpha = 1/157$.

III. PERFORMANCE OF SPREADING SCHEMES FOR COLLUDERS TRACING

Taking the two fingerprint lengths of Tardos-Skoric fingerprints with $n = 1000$ users and a probability of accusing innocent users set to $\varepsilon_1 = 10^{-3}$, we can trace a maximum of $c_0 = [4,6]$ colluders [6]. In this section, we address colluder tracing performance by first emulating video embedding and attacks thanks to a BSC, and then by simulating the realistic embedding (alpha blending and darken attack). To trace the colluders, we used the Nearest Neighbor Search (NNS) decoder for its higher tracing rate and lower complexity [21].

To analyse the impact of spreading scheme for colluders tracing, the fingerprint k is spread and noised over a BSC with error probability p before a majority vote collusion attack is performed, as illustrated in Figure 5(a).

The performance over the BSC is illustrated in the upper graph of Figure 6: we observe that colluders tracing is much improved by the proposed joint scheme compared to the state

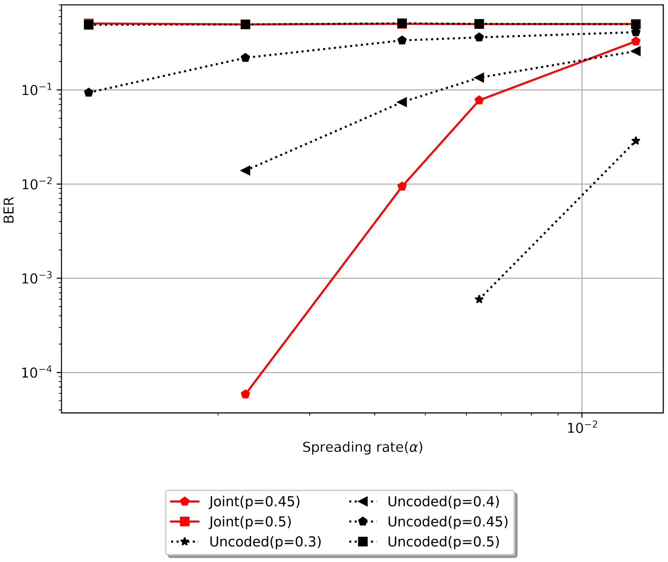
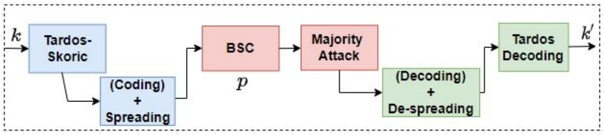
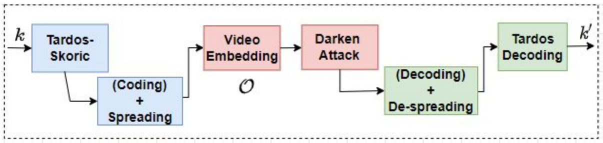


Figure 4: Trade-off between BER and spreading rate for the joint and uncoded scheme with error probability $p \in [0.05, \ldots 0.5]$ for BSC.



(a) Majority attack



(b) Darken attack

Figure 5: Simulation model for colluders tracing with $k = [1440, 2880], n = 1000$ and $\varepsilon_1 = 10^{-3}$ for the uncoded and the joint coding and spreading schemes: (a) Majority vote attack over BSC (b) Darken attack on video with FFMpeg and alpha blending embedding.

of the art uncoded spreading scheme, even when binary errors are higher than $\pi = 2 \times 10^{-1}$.

In the realistic setup, the watermark image is embedded into an open source $1080p$ video Tear of Steel [22]. The watermarked video is created using blending filter of the FFMpeg with alpha channel as opacity. A darken attack using FFMpeg is performed to create an illegal copy of a video as explained in [Mode:B and Table V in [14]]. The model is illustrated in Figure 5(b). In the simulation, we also consider two fingerprint lengths and we let the opacity range from 0.90 to 0.99. The simulation results are depicted in the lower graph of Figure 6. As the opacity increases close to 1 (thus decreasing the SNR), the performance between the 2 schemes becomes equivalent for both fingerprint lengths. However, for lower opacities (higher SNR), the joint scheme still outperforms the uncoded spreading scheme.

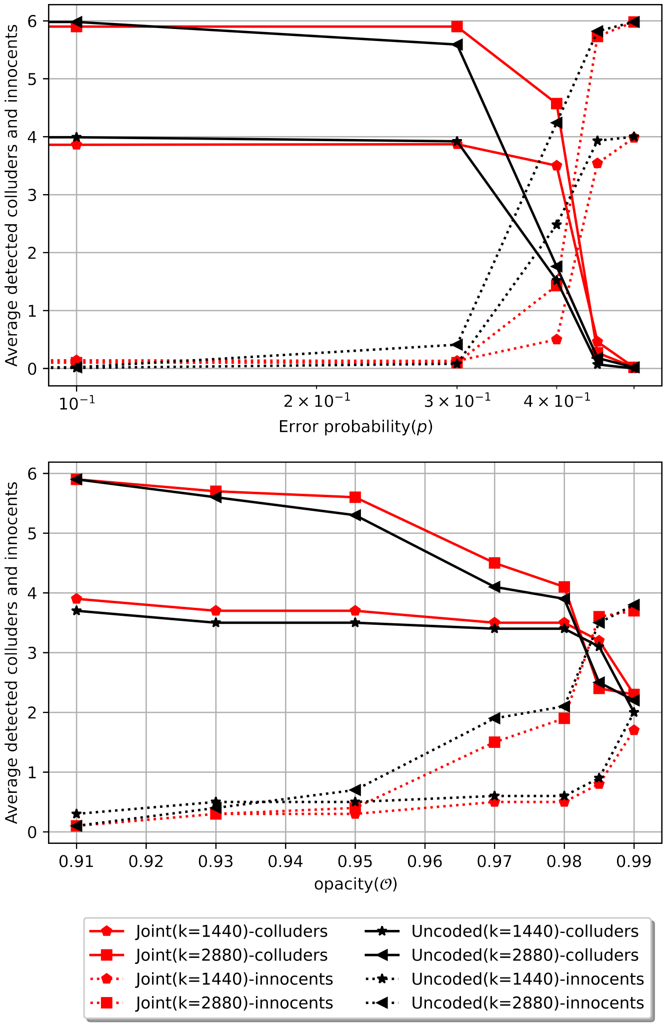


Figure 6: Results for the two simulation models of colluders tracing: The upper part is for the majority vote over BSC, while the plot below is for darken attack on the video with FFMpeg.

IV. CONCLUSION AND FUTURE WORK

Tardos-Skoric codes are used to identify the colluders who took part in the collusion to unlawfully redistribute pirated copies of multimedia contents like e.g., videos. Discreetly watermarking the videos with these codes implies a very low SNR. Spreading schemes on Tardos-Skoric codes improve the SNR at the cost of reducing the Tardos-Skoric code length and the tracing performance. In this article, we proposed to combine error correcting codes with pseudo-random spreading to improve the colluder tracing performance. Firstly, we analyzed the trade-off between the spreading rate and the bit error rate on the fingerprint code. We then estimated the performance of the proposed joint convolutional code and random spreading compared to the uncoded random spreading scheme. Performances were obtained first on a 360p image over a binary symmetric channel with a majority vote attack, and then on a 1080p video with Discrete Wavelet Transform embedded using alpha blending with a darken attack. The performance results in terms of colluder tracing showed that the proposed joint scheme outperforms the uncoded one. Perspectives to this work include the use of more powerful error correction coding schemes to be jointly combined with random spreading.

REFERENCES

[1] Y. Uchida, K. Takagi, and S. Sakazawa, "Fast and accurate content-based video copy detection using bag-of-global visual features," in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2012, pp. 1029–1032.

[2] I. Sayahi, A. Elkefi, and C. Ben Amar, "Join cryptography and digital watermarking for 3D multiresolution meshes security". In: 19th International Conference on Image Analysis and Processing, ICIAP 2017. Springer Verlag. 2017, pp. 637–647.

[3] P. Bas, T. Furon, and F. Cayre, "Practical key length of watermarking systems," in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2012, pp. 1769-1772.

[4] F. Chaabane, M. Charfeddine, and C. Ben Amar, "The impact of error correcting coding in audio watermarking". In: 2011 3rd International Conference on Next Generation Networks and Services (NGNS). 2011, pp. 90z-95, DOI:10.1109/NGNS.2011.6142556.

[5] G. Tardos, "Optimal probabilistic fingerprint codes," in Symposium on the Theory of Computing, 2003, pp 1–24, DOI:10.1145/1346330.1346335.

[6] B. Skoric, S. Katzenbeisser, and M. U. Celik, "Symmetric tardos fingerprinting codes for arbitrary alphabet sizes," Cryptology ePrint Archive, Paper 2007/041, 2007.

[7] A. Gutub, "Boosting image watermarking authenticity spreading secrecy from counting-based secretsharing," CAAI Transactions on Intelligence Technology, vol. 8, pp. 440–452, 2022.

[8] A. Kuznetsov et al., "Adaptive pseudo-random sequence generation for spread spectrum image stenography," in IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, pp. 161–165.

[9] Y. Huang, B. Niu, H. Guan, and S. Zhang, "Enhancing image watermarking with adaptive embedding parameter and psnr guarantee," IEEE Transactions on Multimedia, vol. 21, no. 10, pp. 2447—2460, 2019.

[10] S. Panchikkil, V.M. Manikandan, and Y-D. Zhang, "A pseudo-random pixel mapping with weighted mesh graph approach for reversible data hiding in encrypted image, Multimedia Tools and Applications, vol. 81, no. 12, pp. 16279–16307, 2022.

[11] R. Venkatesan and M.H. Jakubowski, "Randomized detection for spread-spectrum watermarking: defending against sensitivity and other attacks [image watermarking applications]," in Proceedings. (ICASSP 05). IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 2, pp. ii/9-–ii12 , 2005.

[12] H. Tribak, Y. Zaz, and H. Kelkoul, "Advanced video watermarking approach based on convolutional encoding : Search for new solution against cinematography piracy traffic," in 2018 6th International Conference on Multimedia Computing and Systems (ICMCS), pp. 1–7, 2018.

[13] Y. Tan et al., "A robust watermarking scheme in ycbcr color space based on channel coding," IEEE Access, vol. 7, pp. 25026–25036, 2019.

[14] A. Rehman, G. Le Guelvouit, J. Dion, F. Guilloud, and M. Arzel, "Dwt collusion resistant video watermarking using tardos family codes," in 2022 IEEE 5th International Conference on Image Processing Applications and Systems (IPAS), vol. 5, pp. 1–6, 2022.

[15] G. Le Guelvouit and S. Pateux, "Wide spread spectrum watermarking with side information and interference cancellation," in Security and Watermarking of Multimedia Contents V. SPIE, 2003, vol. 5020, pp. 278–289.

[16] R. Kumar and J. Yadav, "Effective compression and decompression coding techniques using multilevel dwt decomposition and dct," International Journal of Signal and Imaging Systems Engineering, vol. 12, no.3, pp. 71-80, 2021.

[17] K. Yu, L. Chen, Z. Fu, Y. Wang, and T. Lu, "A coding layer robust reversible watermarking algorithm for digital image in multi-antenna system," Signal Processing, vol. 199, pp. 108630, 2022.

[18] Md. Ahasan Kabir, "An efficient low bit rate image watermarking and tamper detection for image authentication," SN Applied Sciences, vol. 3, no. 4, pp. 400, 2021.

[19] J.R. Hernandez, J.F. Delaigle, and B. Macq, "Improving data hiding by using convolutional codes and soft-decision decoding". In: Security and Watermarking of Multimedia Contents II. vol. 3971, SPIE. 2000, pp. 24–47.

[20] A. Bensky, "Chapter 9 - introduction to information theory and coding," in Short-range Wireless Communication, Alan Bensky, Ed., pp. 211–236. Newnes, third edition, 2019.

[21] T. Laarhoven, "Nearest neighbor decoding for tardos fingerprinting codes," Proceedings of the ACM workshop on information hiding and multimedia security, pp. 182-187, 2019.

[22] Blender Foundation, "Tears of steel: Open movie free to share and show 2012," in https://mango.blender.org/download/, retrieved: Feb, 2024.