AI Enabled: A Novel IoT-Based Fake Currency Detection Using Millimeter Wave (mmWave) Sensor

Fahim Niaz[1,1], Jian Zhang[2,1*], Muhammad Khalid[3,2],
Kashif Naseer Qureshi[4,3], Yang Zheng[5,1], Muhammad Younas[6,1],
Naveed Imran[7,1]

[1*]School of Computer Science, Wuhan University, Wuhan,China.
[2]School of Computer Science, University of Hull, Hull,UK.
[3]Department of Electronic and Computer Engineering, University of Limerick, Limerick, Ireland.

*Corresponding author(s). E-mail(s): jzhang@whu.edu.cn;
Contributing authors: notify.fahim@outlook.com; m.khalid@hull.ac.uk; KashifNaseer.Qureshi@ul.ie; zh.yang@whu.edu.cn; younas@whu.edu.cn; naveed.imran@whu.edu.cn;

Abstract

In recent years, the significance of millimeter wave sensors has achieved a paramount role, especially in the non-invasive and ubiquitous analysis of various materials and objects. This paper introduces a novel IoT-based fake currency detection using millimeter wave (mmWave) that leverages machine and deep learning algorithms for the detection of fake and genuine currency based on their distinct sensor reflections. To gather these reflections or signatures from different currency notes, we utilize multiple receiving (RX) antennae of the radar sensor module. Our proposed framework encompasses three different approaches for genuine and fake currency detection, Convolutional Neural Network (CNN), k-nearest Neighbor (k-NN), and Transfer Learning Technique (TLT). After extensive experiments, the proposed framework exhibits impressive accuracy and obtained classification accuracy of 96%, 94%, and 98% for CNN, k-NN, and TLT in distinguishing 10 different currency notes using radar signals.

Keywords: Millimeter Wave, Fake Currency, Machine learning, Deep Learning, Signal Processing

1 Introduction

In the global march towards modernization, the allure of new technologies remains undeniable. These advancements have simplified and enriched daily life for many. However, there's a downside, some people misuse these new technologies for harmful reasons. The illicit production of fake currency, facilitated by sophisticated technology, has burgeoned into a lucrative underhand enterprise. Currently, there are 180 distinct currencies circulated worldwide, each characterized by its unique security attributes and dimensions (1). Such features facilitate the identification of a note's nation of origin and its value (2), Nasser et al. (2021). Nevertheless, the rampant rise in currency counterfeiting poses a pressing concern across nations. With the fake notes bearing an uncanny resemblance to authentic ones, distinguishing the genuine from the fraudulent has become a formidable challenge for the global community.

Wireless sensing with broadband signals has established Chouat et al. (2023) its worth in detecting and identifying different materials. For example, Ghiri and Entesari (2019) demonstrated non-contact chemical sensing using ultra-wideband (UWB) pulses, relying on the unique dielectric properties of materials. Millimeter-wave (mmWave) signals, another high-frequency pulse, were utilized to understand non-dispersive and non-magnetic substances by gauging their complex permittivity Vakili et al. (2015). By comparing signals received with and without dielectric slabs, material properties were inferred from perceived signal distortions Tu et al. (2020). When moving to even higher frequencies, the capabilities of broadband mm-wave systems enhance multiple sensing applications. Techniques like remote sensing have been applied to detect minor object vibrations using mm-wave signals, capitalizing on the micro-Doppler effect Björklund et al. (2012). Moreover, THz frequencies are promising for high-precision spectroscopy, where a broad-ranging detector can spot various molecules in a unified manner Jamali et al. (2019). Additionally, with enhanced resolution at diminutive wavelengths, mm-wave radars have proven adept at gesture recognition Hazra and Santra (2018). Several factors, including the thickness of an object, its dimensions, contaminants, and reflections from nearby testing equipment, might influence the signals received in radar and sensing applications. This can introduce a degree of ambiguity in detection outcomes. To address this, one can conduct multiple measurements on the subjects being tested and employ supervised machine learning to categorize based on the amassed data sets. These learning mechanisms can pave the way for smart radars and sensors by identifying consistent patterns in the collected data. As a case in point, applications like heart rate monitoring Saluja et al. (2019), observing human movement patterns and micro-Doppler distinctions Zhang and Cao (2018), pinpointing multiple objects at equal distances from a radar Sarkar and Ghosh (2019), and material categorization at 77-81 GHz Weiß and Santra (2018) have effectively harnessed supervised learning techniques.

In this research, we explore the mmWave Frequency-Modulated Continuous Wave (FMCW) radar equipped with multiple antennas to distinguish signal variations reflected from fake and genuine banknotes. Each receiving antenna functions as an RX channel, generating four pairs of real and imaginary signal sets. Utilizing these signals, we proposed a framework of three distinct methodologies for discriminating between fake and genuine banknotes: deep learning Convolutional Neural Network (CNN);

machine learning k-Nearest Neighbors (k-NN) using different statistical features; and a transfer learning model called AlexNet. In the CNN model, signals from multiple reception channels in both time and frequency domains are visualized as scalogram images using CWT. These images then serve as input to the CNN model, which teases out specific scalogram features to categorize the currency in terms of fake and genuine. For the machine learning k-NN model, we pinpoint ten standard features from the time and frequency domain signals and employ a k-NN model with optimized 'k' values. Finally, in the transfer learning method, the AlexNet model processes scalograms of time and frequency domain signals to extract significant features for categorization purposes. Additionally, we fine-tune each classification model's parameters to enhance accuracy. This designed framework is put to the test against five fake (fake-5, fake-10, fake-20, fake-50, and fake-100) and five authentic (genuine-5, genuine-10, genuine-20, genuine-50, and genuine-100) currency denominations.

The primary contributions of this research are as follows:

- To our understanding, this research is the ubiquitous, contactless, and innovative effort to explore mmWave RF signals for fake currency detection.
- We develop a range of sophisticated algorithms that extract salient patterns from radar signals, further refining the approach to scalogram generation.
- This research proposed a framework that aligns the time and frequency domain signals of FMCW radar with multiple receiving channels, and applies machine and deep learning techniques, specifically CNN and transfer learning to detect fake currency.
- We extract a compact set of ten predefined features, enabling the differentiation of various banknotes through the conventional machine learning technique of the k-NN classifier.

The rest of the paper is organized as: Section 2 discusses related work done with mmWave sensors in different areas. Section 3 gives the detailed designs of the proposed framework and how we put things into action. Sections 4 and 5 cover how we collected data and the methods we used to extract radar features. Sections 6 and 7 explain the setup we used for experiments and how we evaluated our framework. Lastly, in Section 8, we discuss the future work that could explore and conclude our findings.

2 Related Work

This study extends upon two distinct domains of prior research: radar-based interactive sensing and material identification through radar sensors. We conduct a comprehensive review of the existing literature in both domains, highlighting the advancements made, and elucidate the innovative aspects of our methodology in the context of fake currency detection.

Radar-Based Interactive Sensing has witnessed notable advancements with the introduction of miniature radar sensors like Soli Lien et al. (2016). These sensors have paved the way for exploring precise motion sensing in human-computer interaction. Notably, Soli has been utilized for detecting micro-gestures, as evidenced by Ens et al. (2018), where such micro-gestures are seamlessly integrated with larger gestures, offering an intuitive input method for a gesture-based Augmented Reality interface. The work by Wang et al. (2016) extensively explores various Soli-detectable micro-gestures, highlighting the sensors' versatility. Radar sensors, known for their advantages such as a small footprint, low power consumption, and fewer privacy concerns compared to alternative gesture-sensing techniques, enable micro-gestural interaction. As a result, these sensors have found integration into everyday consumer devices, exemplified by their incorporation into devices like Google's Pixel 4 smartphone and the Nest Hub smart display Eckhardt (1971). Furthermore, radar technology has been explored for material and object identification. For example, Cubesense Yang and Zhang (2021) supports radar interactions based on corner reflectors but falls short in distinguishing between different corner reflectors and objects.

Prior research, as demonstrated by Yeo et al. (2016), has shown the capability to detect and classify various objects using radar sensors, introducing context-aware and tangible applications. However, these systems have limitations, as they can only differentiate materials at a fixed distance from the sensor and rely on changes in material properties. The research conducted by McIntosh et al. (2017) utilized an array of microwave Doppler sensors beneath a table, but this approach requires substantial setup space and multiple antennas, making it impractical for everyday use. An alternative proposed by Arakawa and Zhang (2021) introduced low-cost origami-based tangible controllers using mm-wave radar sensors but did not involve the identification of diverse controllers. In our research, we utilize a single 77-81 GHz radar sensor to distinguish between counterfeit and genuine banknotes in a desktop setup. Additionally, Zhao et al. (2019) demonstrated the identification and tracking of human participants through point cloud data on millimeter-wave radar, while Hsu et al. (2019) achieved identification using RF reflections from human participants with high accuracy via a 5.46-7.25 GHz FMCW radio. The research outlined in these papers underscores radar's potential to support human-computer interaction and object/material identification at a fixed distance Yeo and Quigley (2017). However, there is a notable gap in prior research concerning the use of custom radar reflectors to identify counterfeit and genuine currency on a tabletop surface where the distance from the radar sensor varies. Our research addresses this gap by leveraging the distinctive properties of radar reflectors.

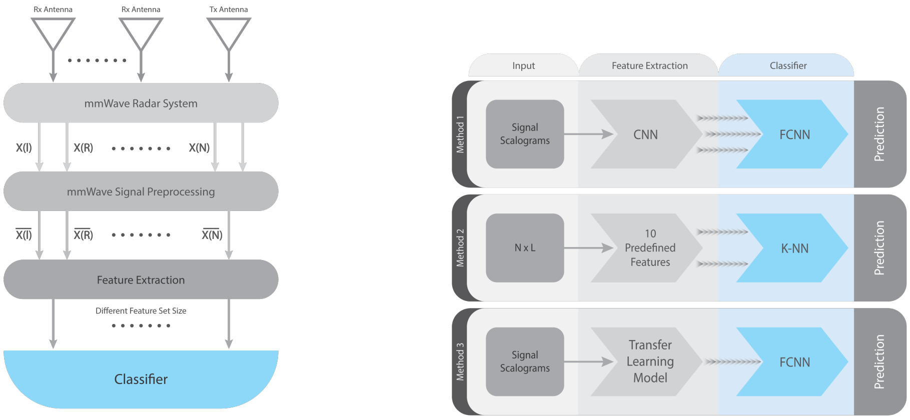
Material detection methods conventionally employ techniques such as optical spectroscopy, large radar, X-ray, and CT/MRI, among others. While these methods yield high-resolution results, their reliance on specialized and bulky instruments makes them costly and confines their use in laboratory settings and critical security applications. In recent years, there has been a growing interest in advancing material identification within diverse contexts Yue and Katabi (2019). Various approaches have explored the use of RF signals, with a particular emphasis on liquid identification. LiquID Dhekne et al. (2018) achieves remarkable accuracy in liquid testing using UWB radar in a specialized setup featuring a unique container. TagScan Xie et al. (2019) classifies liquids by analyzing phase and RSS changes of RFID signals that permeate the target. In subsequent developments, TagTag utilizes the impedance change of RFID tags attached to the target, enabling the simultaneous sensing of multiple targets. RFIQ Ha et al. (2020) exploits electromagnetic interactions between RFID tags on containers and the enclosed materials to assess food quality. TwinLeak Guo et al. (2019) employs RFID for detecting liquid leakage without specifying the types of liquids. WiFi signals have also been employed for material sensing, exemplified by WiMi Feng et al. (2019), which applies a concept similar to TagScan Xie et al. (2019) on standard WiFi devices for liquid identification.

In the domain of suspicious object detection, Wang et al. (2018) introduces a system that identifies liquids and metals, among other objects. Strobe uses a WiFi receiver buried in the soil to sense soil moisture while employing three mutually perpendicular receive antennas (constructed from commodity WiFi cards) to recognize materials Corradini et al. (2023). Notably, the sole work to date utilizing reflection signals on WiFi for material recognition. Millimeter-wave radios, including dedicated radar and networking devices citeqayyum2022assessment, has been applied to object imaging and recognition. RadarCat utilizes Google Soli to interact with targets but distinguishes different objects of the same material type as distinct materials. RSA Zhu et al. (2015) focuses on imaging with 60GHz radios but requires well-separated and independently moving Tx and Rx components. Ulysses improves upon RSA by utilizing a single device, although it still demands precise radio movement and is less suitable for handheld mobile scenarios.

In contrast to existing works, our proposed framework repurposes a single commodity mmWave networking device, harnessing reflection signals to extract explainable and distinguishable features for the sensing of counterfeit and genuine currency.

3 Framework Overview

mmWave radars are better than other sensor types due to their compact size, making them suitable for integration into mobile phones Kwon et al. (2021) and small handheld devices. Unlike vision sensors, radars offer enhanced privacy and are more user-friendly. Also, these compact radars are energy-efficient compared to many other sensor types. Building on these advantages, our proposed model employs a readily available FMCW radar with multi-receiver channel, to capture the signature reflected from both fake and genuine banknotes. Unlike traditional continuous wave (CW) sensors, FMCW sensors ascertain the target range R by emitting a continuous frequency-modulated signal, commonly known as a chirp, with a sweeping bandwidth B. To extract coherent samples in both the time and frequency domains, the received (RX) signal is subsequently converted downward. These samples encapsulate the cumulative attributes of the currency, reflecting its transmission and reflective properties. The mmWave radar signal's reflectivity is influenced by the currency properties and hidden features, such as composition, distinct texture, embedded security threads, and other common security features in banknotes. Similarly, hidden attributes within the currency also influence the absorbed signal strength. Notably, genuine banknotes tend to exhibit stronger signal reflections than their counterfeit counterparts. As such, based on these currency properties, features of the received signals, like mean, standard deviation, and power spectral density, fluctuate. We utilize these unique variations present in the signals of the time and frequency domains. from different banknotes as key indicators to distinguish between genuine and fake notes using mmWave radar. In Fig. 1, our proposed



(a) Radar Signal Processing (b) Proposed Framework for Currency Detection

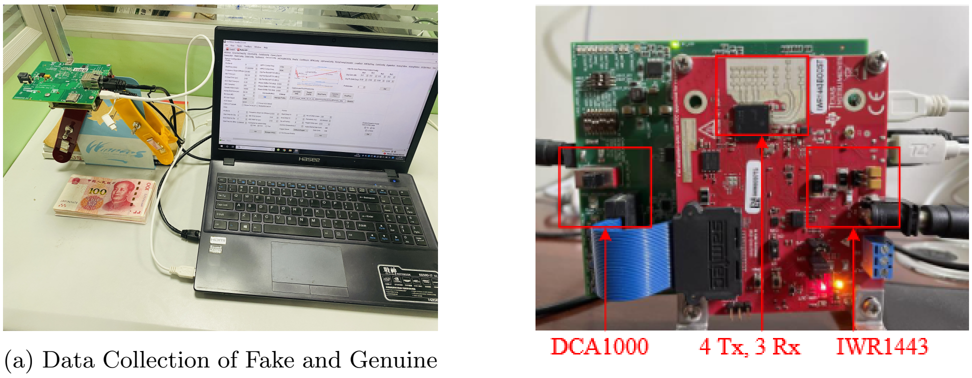
Fig. 1: Fig. 1a shows Signal processing of mmWave sensor and Fig. 1b indicates the proposed framework for fake currency detection

framework for classifaction integrates input from N number of RX channels. The system outputs predictions regarding the authenticity of currency, classifying it as either fake or genuine through the classification network. The mmWave radar's TX antenna transmits FMCW chirp signals, with N RX antennas capturing the reflected signals. Each signal undergoes down-conversion, resulting in both real (R) and imaginary (I) signal components. Afterward, an analog-to-digital converter (ADC) digitizes all N signals, which are then sent to a computer for in-depth analysis. The currency classification methodology involves three distinct strategies, as illustrated in Fig. 1b. The first approach employs the CNN model for classifying the target currency based on received signals. we generate refined signal scalograms for each note using continuous wavelet transform (CWT) and feed them to the CNN model. In the second approach, we derive ten predetermined features (Mean, Median, Max, Min, Standard Deviation, Variance, Peak-to-Peak (Range), Root Mean Square (RMS), Kurtosis, and Skewness) from the FMCW reflected signals to train the machine learning k-NN algorithm. Finally, a transfer learning technique (TLT) based on the AlexNet model with the CNN model is used to classify fake and genuine currency notes using signal scalograms.

4 Data Collection

The data collection process required a carefully orchestrated procedure to capture a wide variety of both genuine and counterfeit currency samples. At the core of our dataset are both genuine and fake banknotes that we sourced directly from a regional Chinese bank. The radar signals are recorded from each genuine and fake note in a controlled tabletop setup as shown in Fig. 2.

we utilize the TI IWR1443 FMCW sensor device, as illustrated in Fig. 2, designed according to the specifications outlined in the TI datasheet (2021). This device consists of three transmission and four receiving antennas. A maximum of two antennas can transmit signals concurrently, and all receiving antennas can receive reflected signals simultaneously. This radar sensor is engineered to cover frequency bands within the 77–81 GHz range. Moreover, it is an all-encompassing chip that incorporates an RF system, ramp generator, integrated memory chip, digital front end, and signal processing unit.



(a) Data Collection of Fake and Genuine Notes

(b) IWR1443 FMCW Radar Module

Fig. 2: Fig. 2a Data collection of fake and genuine notes using mmWave sensor and Fig. 2b shows the Texas Instruments (TI)IWR1443 FMCW Radar Module

Delving deeper into its architecture, power amplifiers (PA) binary phase modulation (BPM) are attached to each transmission antenna (TX) in the RF system. The ADC, mixer, IF filtering, and low-noise amplifier (LNA) are linked to each receiving antenna (RX), which then proceeds to a decimation phase. The ramp generator, a vital component, seamlessly modulates the input voltage of a voltage-controlled oscillator (VCO). This modulation process induces a frequency shift in a local oscillator. Following this, an RF synthesizer generates a wave, which is subsequently refined by a 4× multiplier to create the necessary ramp chirp waveform. The echo, captured by the RX antenna, undergoes coherent down-conversion to an intermediate frequency (IF) at the mixer. This process leverages the same chirp and finally undergoes low pass filtering (LPF). To derive the real (R) and imaginary (I) components of the beat signal, a 90° phase shifter is employed. These analog beat signals are then individually digitized by two distinct ADCs, subsequently channeling them to the processing unit for further refinement. The samples collected is contingent upon the count of active RX channels. Hence, N RX channels will yield N pairs of R and I beat signals, symbolized as $X(R)1$, $X(I)1$, $X(R)2$, $X(I)2$, ... , $X(R)N$, and $X(I)N$. Conventionally, the ADC output for the beat signal is structured and saved as a series of complex vectors, effectively forming a complex matrix X. This matrix has dimensions equivalent to (the count of channels × the sample count per frame), which is represented as $N \times L$. Here,

N signifies the number of active RX channels, and L indicates the sample count within each captured frame. Thus, X can be characterized as $X[n, l] = X[l](R)n + jX[l](I)n$, where 'n' falls within 1, N indicating the antenna index and 'l' within 1, L pointing to the time index, showcasing the dimensions of the incoming raw signal. For every RX channel, the signals undergo further normalization, setting their mean to zero and adjusting their standard deviation to one. This refined matrix, X, becomes the cornerstone for currency classification in the methodologies we've implemented.

5 Feature Extraction of mmWave Radar Signals

5.1 Convolutional Neural Network (CNN)

For time-series data analysis and pattern recognition, deep learning algorithms have surged in popularity, and play a vital role in extracting features Xia (2020). CNNs outperform other machine learning paradigms by virtue of their inherent capability to autonomously extract spatial-temporal features from datasets, eliminating the need for manual feature extraction. Within the realm of multi-channel sensor, spatial features characterize the interrelations among signals captured via synchronized channels. Conversely, 'temporal features' articulate the correlations among ADC time samples, capturing the material's radial attributes.

As convolutional layers traverse the input signal, they discern and isolate distinctive features. These features, once extracted, are then utilized to instruct a fully connected neural network for carrying out classification tasks. For our study, we processed signal scalograms of both fake and genuine currency notes (800x300) through our CNN for intricate feature extraction. This process is visually represented in Table 2. The images then pass through a fully connected layer dedicated to currency differentiation. The classification structure we propose encompasses three sequential convolutional layers, succeeded by a flattening layer. This latter layer restructures the data, This ensures compatibility with the subsequent fully connected neurons. we set 64 filters in the initial 2D convolutional layer, each measuring 3x3, while the subsequent layer possesses 32 filters of 2x2 dimensions. Through empirical analysis, we optimized the network parameters to maximize classification precision, with detailed configurations outlined in Table 1

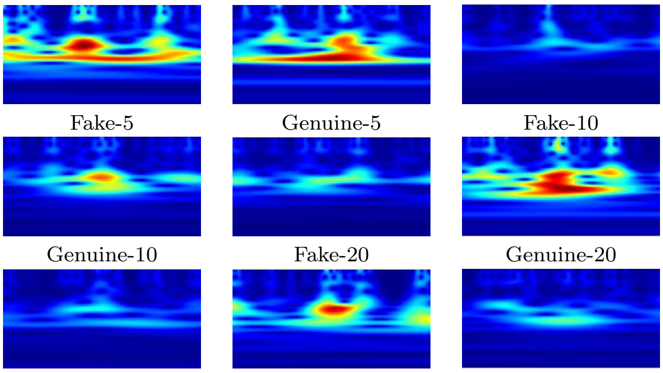
5.2 Machine Learning

The k-NN algorithm operates under supervised learning and classifies an input based on the most common class among its k closest data samples. Despite its simplicity, k-NN often yields impressively accurate classification results. Indeed, it has been established that as both the training samples and k approach infinity, k-NN converges to emulate the Bayesian classifier Theodoridis (2015). In this methodology, we employ a distinct strategy to train k-NN, relying on ten features: mean, median, max, min, standard deviation, variance, peak-to-peak (range), root mean square (RMS), kurtosis, and skewness derived from the acquired signals. Each collected raw data instance possesses dimensions of $N \times L$, where N indicates the number of RX antennas, and

Table 1: CNN Architecture for the Proposed Framework

Layer	**Parameters**	**Value**
Input Shape	-	300*800*3
2D-CNN	No. of filters Filter_Size Activation_Function	64 3*3 ReLu
2D-CNN	No. of filters Filter_Size Activation_Function	32 2*2 ReLu
2D-CNN	No. of filters Filter_Size Activation_Function	16 2*2 ReLu
Flatten	-	-
FCDN	Classification_Output Activation_Function	10 SoftMax

Table 2: Reflected Signal Scalograms from Each Currency Note



Fake-5 Genuine-5 Fake-10

Genuine-10 Fake-20 Genuine-20

Fake-50 Genuine-50 Fake-100

the number of samples within each frame is denoted by L. The raw sensor data undergoes careful processing to extract the ten features. For a single currency sample of one antenna, the features $1 \times L$ dimensions. The predefined features are assessed using this vector, producing an improved feature vector with dimensions 1×10. Hence, each currency signal produces N feature from every received frame of the RX channel, resulting in a dimension of $N \times 10$. As a result, The comprehensive feature table is structured, with rows denoting samples and columns specifying particular features. To improve the accuracy of classification, the parameter k can be fine-tuned further.

5.3 Transfer Learning Technique

We utilize the AlexNet Krizhevsky et al. (2012) transfer learning model with simple CNN to classify between fake and real currency detection. In our research framework for detecting fake currency using mm-wave radar, we leveraged the capabilities of AlexNet, a renowned pre-trained model. While AlexNet was originally architected for large-scale image classification, its deep convolutional layers offered the ability to extract hierarchical features from images making it a prime solution for our task. To adapt AlexNet for our specific currency classification problem, we refined the output layer to distinguish between genuine and fake currency. Given the distinctive nature of the mm-wave signal, we make signal scalograms using CWT, and data augmentation strategies were introduced to enhance the dataset's diversity and ensure model generalization. Importantly, rather than training the model from scratch, we retained the patterns learned by the initial layers of AlexNet. However, to capture the specific features of fake currency in the signal scalograms, we fine-tuned the model's deeper layers. This strategy of harnessing pre-existing knowledge combined with targeted training proved effective.

6 Experimental Setup

For the experiments, we used the IWR1443 mmWave FMCW radar sensor module from TI (2021), which we configured to function within the 77–81 GHz frequency band. The radar was strategically positioned at the tabletop, to gather experimental data. Following our setup, both genuine and fake banknotes were systematically positioned in the radar's interaction zone to collect signal samples. As per Balanis (2011), the mmWave radar distance can be estimated using the formula $2d^2/\lambda$, where 'd' symbolizes the maximum linear dimension, and 'λ' represents the wavelength of the sensor. The dimension of the MIMO is approximately 4.6λ. Given the operational frequency of the radar is set to 77 GHz, the wavelength is roughly 0.42 cm. This translates to a distance of about 20.5 cm. Given these metrics, the currency lies in an interaction area between the radar's near-field and far-field regions, with respect to the MIMO array. The radar module in use possesses an azimuth beamwidth of $\pm 50\circ$ and an elevation beamwidth of $\pm 20\circ$, defined by a 6 dB signal drop from the center. As our identification hinges on the unique RF signature of the reflected signals, any potential variations between near and far fields shouldn't impede the signature, especially since the currency notes maintain a proper distance from the mmWave within its interaction zone. Our designated interaction zone for the experiments measures 20 × 20 cm. This ensures that the zone surpasses the radar's illuminative reach, optimizing radar signal acquisition.

In the experimental setup, illustrated in Fig. 2a, we engaged one TX channel and four RX channels. This configuration is consistently employed for all banknote samples. It's worth noting that any signals introduced by the table's surface could be factored into the measurements. However, such interference is likely dismissed by the classifier and doesn't notably skew the experimental results, as alluded to in Bishop and Nasrabadi (2006). Data collection spanned multiple sessions over a week, ensuring a diverse set of environmental conditions during collection. For each currency note the

Algorithm 1 Fake and Genuine Currency Detection using mm-Wave

```
Input: $RFS$ - Radar Frequency Signal
Output: $Prediction$ - Fake or Genuine
Step 1: Preprocess the received signal
    $RFS_{\text{detrended}} \leftarrow \text{DetrendSignal}(RFS)$
    $RFS'_{\text{denoised}} \leftarrow \text{RemoveNoise}(RFS_{\text{detrended}})$
    $RFS'' \leftarrow \text{ApplyHighPassFilter}(RFS'_{\text{denoised}})$
Step 2: Create signal scalograms for feature extraction
    $SI \leftarrow \text{ScalogramImages}(RFS'')$
Step 3: Extract features from scalograms
    $Features \leftarrow \text{FeatureExtractionMethod}(SI, \text{method1}, \text{method2}, \text{method3})$
Step 4: Use Proposed framework model for prediction
    $Prediction \leftarrow \text{PredictFakeGenuine}(Features)$
Output: $Prediction$
```

data sample is separated into two segments: one for training data samples and the other for testing. Notably, the testing set is entirely new to the classifier, ensuring a true test of its performance. Within these training and testing datasets, the physical samples were further subdivided. For instance, the training segment was arbitrarily split into three sub-segments. In every data collection session, a sample was placed within the interaction area for a specific duration and then subsequently removed. In subsequent sessions, the sample was reintroduced with varied placements to randomize conditions. To enrich the robustness of our dataset, each physical currency sample underwent three distinct measurements. These were captured with varying, random orientations to ensure a comprehensive capture of potential features. Throughout this process, a uniform measurement approach was adhered to for all ten currency denominations. This meant that for any given currency type, the alterations in orientation along the vertical axis remained consistent across samples. After each orientation measurement, the currency was randomly rearranged within the interaction zone, even if it was the same physical sample, to enhance variability.

In this research, the frequency peak power of FMCW radar operates is 12 dBm, for data collection from diverse banknotes. The starting frequency of the FMCW radar chipset is, f_{start}, which is started at 77 GHz, sweep bandwidth, B is set at 4 GHz, and the IF bandwidth of radar is 15-MHz. The duration of chirp is, T_c, we opted for is 40 μs, translating to a ramp chirp rate, S, of 100 MHz/μs. Consequently, It is determined by the maximal discernible area $\text{Range}_{\text{max}} = (\text{IF}_{\text{max}} \times c)/(2 \times S)$, where IF_{max} signifies the maximal supported IF bandwidth, c, and S denotes the speed of light and ramp chirp rate. This configuration permits a substantial area of up to 22.5 m. We specified the ADC sampling rate at 18.75 MHz and configured the frame to envelop a lone chirp, resulting in a strike range R_d, of 9.6 m. The subsequent count of time samples is $\left(\frac{2 \times R_d \times B}{c}\right) = 256$, aligning with the time samples per frame, L (considering the frame comprises solely one chirp). The information from the four RX channels is amalgamated into a matrix sized 4×256, serving as the primary input for our detection methodologies. Our focus settled on ten distinct banknotes: fake-5, fake-10, fake-20, fake-50, fake-100, genuine-5, genuine-10, genuine-20, genuine-50, and genuine-100. This selection ensures a broad examination of notes, each presenting varying reflective properties, refractive indexes, thicknesses, and dielectric constants. While gathering samples, we are meticulous in ensuring that each note's orientation and placement under the radar sensor is randomized. This approach amplifies the data's inherent variability, which proves instrumental in refining the classification network for real-world applications.

7 Evaluation

In our research, we have developed a fully integrated prototype for fake and genuine currency notes, employing a commercial off-the-shelf (COTS) sensor. Importantly, we've made no modifications to the hardware or software of the original sensor. The underlying algorithms are made using Python 3 and Pytorch 1.5, executed on a MacBook equipped with a 2.4GHz Intel Core i5 processor and 8GB of RAM, running the mac OS operating system. This setup is attached to the DCA1000EVM via an Ethernet connection. Table. 2 displays an example of the obtained time-frequency domain signal scalograms, representing the samples extracted from the four RX channels of the sensor. From this representation, it's visible that each currency note responds differently to an identical transmitted waveform, positioning it for classification using our varied proposed methodologies. Table 3 shows the classification performance of the proposed framework. To discover the efficacy of our classification schema, we've delineated the following evaluative metrics:

Table 3: Proposed Framework Classification Performance

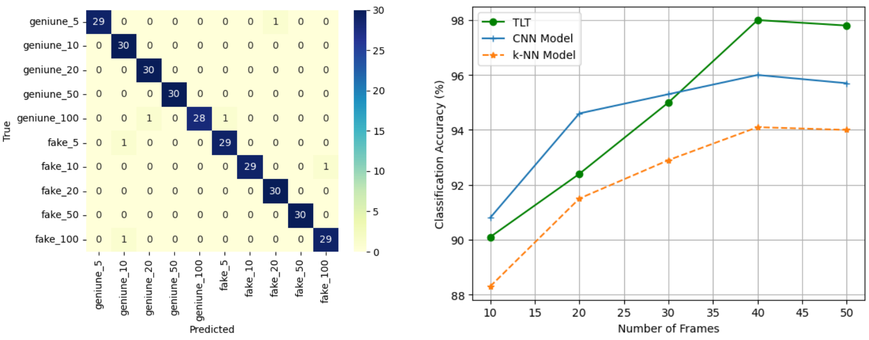
Classifiers	**Accuracy(%)**
Deep Learning	96%
Machine Learning	94%
Transfer Learning	98%

- Accuracy: Denoted as the proportion of correctly discerned samples in relation to the entirety of samples.
- Precision: Characterized as the fraction of accurately identified counterfeit and legitimate notes relative to all the notes categorized as such.
- Recall: Defined as the proportion of accurately pinpointed counterfeit and authentic notes in relation to the complete set of actual counterfeit and legitimate notes.
- F1-score: This metric serves as a harmonized measure of precision and recall, offering a balanced viewpoint of both aspects.
- False alarm rate (FAR). FAR is the probability of identifying fake notes as genuine notes.
- Missing alarm rate (MAR). MAR is the probability of identifying a genuine note as a fake note.

Method 1 is based on a deep learning approach, our dataset consists of signal scalograms and is partitioned, allocating 80% for training and the residual 20% for testing, ensuring that the test segment has not been previously exposed to the CNN classifier. The training dataset is further split into two parts, designating 80% for iterative training and the remaining 20% for validation. The dataset undergoes five rotations, and each rotation's training is reinforced using five-fold cross-validation. Ultimately, the model culminated in a fully connected layer with a softmax function to classify the ten distinct currency notes. This method achieved a commendable classification accuracy of 96%. using method 2, a k-NN Classifier, we utilized 10 pre-defined features I-e. mean, median, max, min, standard deviation, variance, peak-to-peak (Range), root mean square (RMS), kurtosis, and skewness. To enhance the classification outcome, the parameter 'k' is varied. The standard practice involves splitting the feature dataset into 80% for training and 20% for testing, incorporating data that has not been previously exposed. With this configuration, in all three scenarios, the highest accuracy is achieved when k = 1, signifying that the training set size is substantial enough to yield closely matching neighbors. The classification accuracy for different scenarios 1–3 is 93.2%, 94%, and 92.1%, respectively.

Table 4: Accuracy of different models w.r.t different distance

Models	D-15	D-20	D-25	D-30	D-35
CNN	95.0	96.2	94.8	88.1	85.0
k-NN	93.2	94.0	92.1	86.3	80.9
TLT	96.5	97.9	95.0	88.7	86.0



(a)

(b)

Fig. 3: Fig.3a shows the confusion matrix for each classification and Fig.3b indicate Number of Frames Vs. Classification Accuracy(%)

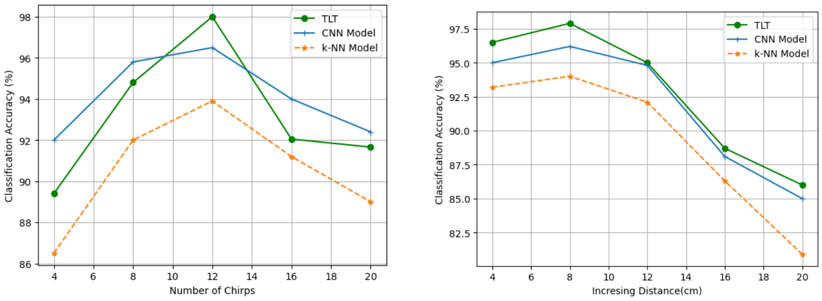
Finally, Using the transfer learning technique(TLT), We adapted the renowned AlexNet model, originally trained on the vast ImageNet dataset, to the task of detecting fake currency using mm-wave radar signal scalograms. The AlexNet architecture, celebrated for its depth, commences with an input layer designed for 227 × 227 × 3 images. It then cascades through five convolutional layers, the first of which employs 96 kernels of an 11×11 size with a stride of four, leading to layers of max-pooling and normalization. Subsequent convolutional layers utilize kernel sizes primarily of 5 × 5 and 3×3 dimensions. The convolutional sequences culminate in three fully connected layers, the first two boasting 4096 neurons each. The original output layer, designed for ImageNet, had 1000 neurons which we adapted for our binary classification task to just two neurons: representing genuine and fake currency classifications. Furthermore, our adaptation included data augmentation techniques specifically optimized for signal scalograms and fine-tuning of the last layers' weights while freezing the initial layers, thus capitalizing on basic feature captures. Training this adapted AlexNet on our radar dataset yielded an impressive accuracy of 98% on the test set, a feat surpassing the results from both the standalone CNN and KNN approaches. Several factors contribute to this success. The inherent depth of AlexNet facilitates the capturing of intricate features, while the foundational weights from a dataset as comprehensive as ImageNet expedite model convergence and reduce the need for extensive training data. By tailoring the architecture's final layers to our task, the model nuanced characteristics of fake currency in radar scalograms. This endeavor underscored the potent combination of deep transfer learning and mm-wave signal scalograms in discerning counterfeit currencies with high accuracy.

Table 5: Accuracy of different models w.r.t to different numbers of chirps

Models	C-04	C-08	C-12	C-16	C-20
CNN	92.0	95.8	96.5	94.0	92.4
k-NN	86.5	92.0	93.9	91.2	89.0
TLT	89.4	94.8	98.0	92.05	91.66

7.1 Ablation Study

We evaluate the effectiveness of the proposed framework for fake currency detection in terms of chirp size, the impact of training data size, and moving people around the radar. Number of Chirps: We conducted a comprehensive performance evaluation of our proposed framework under various numbers of chirps. Specifically, we examined the impact of setting the number of chirps to 4, 8, 12, 16, and 20 on the detection accuracy for the proposed framework, among three, the TLT algorithm results are 89.44%, 94.8%, 96.00%, 92.05%, and 91.66%, respectively. The results in Table 5 and Fig. 4a revealed interesting patterns in accuracy concerning the number of chirps. When the number of chirps is relatively low, such as in the case of 4, we observed an increase in accuracy with the addition of more chirps. The peak accuracy was achieved when the number of chirps was set to 12 and 16. However, beyond this point, as the number of chirps continued to increase, we observed a decrease in accuracy. One potential explanation for this phenomenon is the concurrent increase in the number of out-of-order packets as the number of chirps grows. Our analysis uncovered that, with 16 chirps, the average out-of-order packet index stood at 3. In contrast, when the number of chirps was extended to 20, the average out-of-order packet index surged to 16. Impact of increasing distance: In our framework, the diverse models we proposed are intrinsically tied to the distance size, a crucial determinant of system performance. As shown in Table. 4 and Fig. 4b, there exists a clear correlation between the note and radar device detection accuracy. Notably, when the distance between the note and the device is relatively small, the system exhibits a rapid increase in accuracy, particularly when the size is between 15 to 20cm. However, once the distance increases from 20cm, the observed loss in accuracy becomes more modest.



(a)

(b)

Fig. 4: Fig.4a shows Number of chirps Vs. Classification Accuracy(%) and Fig.4b indicates Increasing Distance(cm) Vs. Classification Accuracy(%)

Maximum frames per sample: We proceed to assess the impact of the number of frames and evaluate by examining the impact on recognition performance. In Fig. 3b, we incrementally increase the number of frames from 10 to 50 per sample. The comprehensive detection accuracy of the proposed framework ranges from approximately 95.5% to 97.8%. In general, employing more frames leads to improved results. More specifically, achieving a higher accuracy is observed when utilizing 40 frames per sample, equivalent to approximately 2 seconds on our current test with a sampling rate of around 20Hz. it is primarily restricted by the file and network I/O of the existing setup. However, an excessive number of frames might introduce larger delays, potentially causing distortions that could compromise accuracy. To strike a balance between accuracy, measuring delay, and computation, we have opted for setting the number of frames per sample to 40 in the proposed framework. This decision is geared towards optimizing for a shorter sensing time, thereby enhancing the user experience and offering more flexibility for the networking aspect in the integrated radar systems.

Moving People around Radar: We assessed the robustness of our framework in scenarios involving the presence of moving individuals in proximity to the radar. To examine this, we introduced 1, 2, 3, 4, and 5 individuals moving around a table. The average accuracy exhibited a decline to 93.18% in the presence of moving individuals, in contrast to the 98% accuracy observed when no individuals were in motion. To further validate our findings, we conducted 1-fold, 3-fold, and 5-fold cross-validations in scenarios with varying numbers of individuals moving around the table. The results indicated average accuracy of 93.66%, 94.39%, and 95.30%, respectively. This effect can be attributed to the introduction of new reflection paths due to the motion of individuals within the radar's range.

8 Conclusion and Future Work

In this study, we utilized signals from a multi-antenna mmWave FMCW radar to distinguish between fake and genuine currency notes. We introduce a framework that encompasses three distinct methodologies for currency detection, leveraging time-frequency radar signals acquired from four *Rx* antennas of a compact mmWave radar module. Our efforts have resulted in a near-optimal classification precision for ten unique currency notes. Notably, we have pioneered an innovative application of a transfer learning model for currency note identification using mmWave radar. The proposed framework achieved a high accuracy of 98% in detecting counterfeit and genuine currency notes. Given its commendable precision, this framework holds tangible potential for real-world, non-invasive counterfeit currency detection, especially when implemented on a Commercial Off-The-Shelf (COTS) device, making it adaptable to any standard radar capable of producing range-Doppler measurements. In future work, endeavors may include expanding the study to incorporate currencies from diverse nations and delving deeper into advanced deep-learning techniques.

References

Know about 180 countries currency. Available at: https://www.eurochange.co.uk/travel/tips/world-currency-abbreviations-symbols-and-codes- (1)

chinese currecny security features. Available at: https://blog.remitforex.com/how-to-identify-counterfeit-rmb/ (2)

Nasser, N., Emad-ul-Haq, Q., Imran, M., Ali, A., Razzak, I., Al-Helali, A.: A smart healthcare framework for detection and monitoring of covid-19 using iot and cloud computing. Neural Computing and Applications, 1–15 (2021)

Chouat, H., Abbassi, I., Graiet, M., Südholt, M.: Adaptive configuration of iot applications in the fog infrastructure. Computing **105**(12), 2747–2772 (2023)

Ghiri, R.E., Entesari, K.: A miniaturized uwb microwave dual-comb dielectric spectroscopy system. IEEE Transactions on Microwave Theory and Techniques **67**(12), 5218–5227 (2019)

Vakili, I., Ohlsson, L., Wernersson, L.-E., Gustafsson, M.: Time-domain system for millimeter-wave material characterization. IEEE Transactions on Microwave Theory and Techniques **63**(9), 2915–2922 (2015)

Tu, W., Yang, Y., Du, B., Yang, W., Zhang, X., Zheng, J.: Rnn-based signal classification for hybrid audio data compression. Computing **102**, 813–827 (2020)

Björklund, S., Johansson, T., Petersson, H.: Evaluation of a micro-doppler classification method on mm-wave data. In: 2012 IEEE Radar Conference, pp. 0934–0939 (2012). IEEE

Jamali, B., Zhou, J., Babakhani, A.: Broadband spectroscopy of materials with an integrated comb-based millimeter-wave detector. In: 2019 44th International Conference on Infrared, Millimeter, and Terahertz Waves (IRMMW-THz), pp. 1–2 (2019). IEEE

Hazra, S., Santra, A.: Robust gesture recognition using millimetric-wave radar system. IEEE sensors letters **2**(4), 1–4 (2018)

Saluja, J., Casanova, J., Lin, J.: A supervised machine learning algorithm for heart-rate detection using doppler motion-sensing radar. IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology **4**(1), 45–51 (2019)

Zhang, R., Cao, S.: Real-time human motion behavior detection via cnn using mmwave radar. IEEE Sensors Letters **3**(2), 1–4 (2018)

Sarkar, A., Ghosh, D.: Detection of multiple humans equidistant from ir-uwb siso radar using machine learning. IEEE Sensors Letters **4**(1), 1–4 (2019)

Weiß, J., Santra, A.: One-shot learning for robust material classification using millimeter-wave radar system. IEEE sensors letters **2**(4), 1–4 (2018)

Lien, J., Gillian, N., Karagozler, M.E., Amihood, P., Schwesig, C., Olson, E., Raja, H., Poupyrev, I.: Soli: Ubiquitous gesture sensing with millimeter wave radar. ACM Transactions on Graphics (TOG) **35**(4), 1–19 (2016)

Ens, B., Quigley, A., Yeo, H.-S., Irani, P., Piumsomboon, T., Billinghurst, M.: Counterpoint: exploring mixed-scale gesture interaction for ar applications. In: Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, pp. 1–6 (2018)

Wang, S., Song, J., Lien, J., Poupyrev, I., Hilliges, O.: Interacting with soli: Exploring fine-grained dynamic gesture recognition in the radio-frequency spectrum. In: Proceedings of the 29th Annual Symposium on User Interface Software and Technology, pp. 851–860 (2016)

Eckhardt, H.: Simple model of corner reflector phenomena. Applied Optics **10**(7), 1559–1566 (1971)

Yang, X., Zhang, Y.: Cubesense: Wireless, battery-free interactivity through low-cost corner reflector mechanisms. In: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, pp. 1–6 (2021)

Yeo, H.-S., Flamich, G., Schrempf, P., Harris-Birtill, D., Quigley, A.: Radarcat: Radar categorization for input & interaction. In: Proceedings of the 29th Annual Symposium on User Interface Software and Technology, pp. 833–841 (2016)

McIntosh, J., Fraser, M., Worgan, P., Marzo, A.: Deskwave: Desktop interactions using low-cost microwave doppler arrays. In: Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 1885–1892 (2017)

Arakawa, R., Zhang, Y.: Low-cost millimeter-wave interactive sensing through origami reflectors. In: CHIIoT@ EWSN/EICS (2021)

Zhao, P., Lu, C.X., Wang, J., Chen, C., Wang, W., Trigoni, N., Markham, A.: mid: Tracking and identifying people with millimeter wave radar. In: 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 33–40 (2019). IEEE

Hsu, C.-Y., Hristov, R., Lee, G.-H., Zhao, M., Katabi, D.: Enabling identification and behavioral sensing in homes using radio reflections. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–13 (2019)

Yeo, H.-S., Quigley, A.: Radar sensing in human-computer interaction. interactions **25**(1), 70–73 (2017)

Yue, S., Katabi, D.: Liquid testing with your smartphone. In: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services, pp. 275–286 (2019)

Dhekne, A., Gowda, M., Zhao, Y., Hassanieh, H., Choudhury, R.R.: Liquid: A wireless liquid identifier. In: Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services, pp. 442–454 (2018)

Xie, B., Xiong, J., Chen, X., Chai, E., Li, L., Tang, Z., Fang, D.: Tagtag: material sensing with commodity rfid. In: Proceedings of the 17th Conference on Embedded Networked Sensor Systems, pp. 338–350 (2019)

Ha, U., Leng, J., Khaddaj, A., Adib, F.: Food and liquid sensing in practical environments using {RFIDs}. In: 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20), pp. 1083–1100 (2020)

Guo, J., Wang, T., He, Y., Jin, M., Jiang, C., Liu, Y.: Twinleak: Rfid-based liquid leakage detection in industrial environments. In: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, pp. 883–891 (2019). IEEE

Feng, C., Xiong, J., Chang, L., Wang, J., Chen, X., Fang, D., Tang, Z.: Wimi: Target material identification with commodity wi-fi devices. In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp. 700–710 (2019). IEEE

Wang, C., Liu, J., Chen, Y., Liu, H., Wang, Y.: Towards in-baggage suspicious object detection using commodity wifi. In: 2018 IEEE Conference on Communications and Network Security (CNS), pp. 1–9 (2018). IEEE

Corradini, F., Fedeli, A., Fornari, F., Polini, A., Re, B., Ruschioni, L.: X-iot: a model-driven approach to support iot application portability across iot platforms. Computing, 1–25 (2023)

Zhu, Y., Zhu, Y., Zhao, B.Y., Zheng, H.: Reusing 60ghz radios for mobile radar imaging. In: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, pp. 103–116 (2015)

Kwon, S., Park, S., Cho, H., Park, Y., Kim, D., Yim, K.: Towards 5g-based iot security analysis against vo5g eavesdropping. Computing **103**, 425–447 (2021)

IWR1443 single-chip 76- to 81-GHz mmWave sensor evaluation module. Available at: https://www.ti.com/tool/IWR1443BOOST (2021)

Xia, Y.: Research on statistical machine translation model based on deep neural network. Computing **102**, 643–661 (2020)

Theodoridis, S.: Machine Learning: a Bayesian and Optimization Perspective. Academic press, ??? (2015)

Krizhevsky, A., Sutskever, I., Hinton, G.E.: Imagenet classification with deep convolutional neural networks. Advances in neural information processing systems **25** (2012)

Balanis, C.A.: Modern Antenna Handbook. John Wiley & Sons, ??? (2011)

Bishop, C.M., Nasrabadi, N.M.: Pattern Recognition and Machine Learning vol. 4. Springer, ??? (2006)