PROCEEDINGS OF SPIE

SPIEDigitalLibrary.org/conference-proceedings-of-spie

# DEMA: decentralized electrical network frequency map for social media authentication

Deeraj Nagothu, Ronghua Xu, Yu Chen

Deeraj Nagothu, Ronghua Xu, Yu Chen, "DEMA: decentralized electrical network frequency map for social media authentication," Proc. SPIE 12542, Disruptive Technologies in Information Sciences VII, 125420B (15 June 2023); doi: 10.1117/12.2663303

SPIE.

Event: SPIE Defense + Commercial Sensing, 2023, Orlando, Florida, United States

# DEMA: Decentralized Electrical Network Frequency Map for Social Media Authentication

**Deeraj Nagothu**[a], **Ronghua Xu**[a], **Yu Chen**[a,*]
[a]Dept. of Electrical and Computer Engineering, Binghamton University, Binghamton, NY 13902

## ABSTRACT

The information era has gained a lot of traction due to the abundant digital media contents through technological broadcasting resources. Among the information providers, the social media platform has remained a popular platform for the widespread reach of digital content. Along with accessibility and reach, social media platforms are also a huge venue for spreading misinformation since the data is not curated by trusted authorities. With many malicious participants involved, artificially generated media or strategically altered content could potentially result in affecting the integrity of targeted organizations. Popular content generation tools like DeepFake have allowed perpetrators to create realistic media content by manipulating the targeted subject with a fake identity or actions. Media metadata like time and location-based information are altered to create a false perception of real events. In this work, we propose a Decentralized Electrical Network Frequency (ENF)-based Media Authentication (DEMA) system to verify the metadata information and the digital multimedia integrity. Leveraging the environmental ENF fingerprint captured by digital media recorders, altered media content is detected by exploiting the ENF consistency based on its time and location of recording along with its spatial consistency throughout the captured frames. A decentralized and hierarchical ENF map is created as a reference database for time and location verification. For digital media uploaded to a broadcasting service, the proposed DEMA system correlates the underlying ENF fingerprint with the stored ENF map to authenticate the media metadata. With the media metadata intact, the embedded ENF in the recording is compared with a reference ENF based on the time of recording, and a correlation-based metric is used to evaluate the media authenticity. In case of missing metadata, the frames are divided spatially to compare the ENF consistency throughout the recording.

**Keywords:** Multimedia Metadata Verification, DeepFake Detection, Misinformation, Social Media, Decentralized ENF Map.

## 1 Introduction

The modern technological advancements in digital applications along with the backbone network architecture have enabled the expansion of online social media companies. With the growth in the number of active participants for each application, the information broadcast online has increased tremendously.[1] Compared to the previous generation of scheduled news broadcasts, social media has allowed for the instantaneous sharing of news with a much wider range of diversified public consumers. On the one hand, with the ease of access and low-cost information broadcast, social media networks have allowed consumers direct access to unmoderated information and maintain social connections with a diverse audience. However, social media can be a double-edged sword

Disruptive Technologies in Information Sciences VII, edited by Misty Blowers, James Holt, Bryant T. Wysocki, Proc. of SPIE Vol. 12542, 125420B
 · 0277-786X · doi: 10.1117/12.2663303

due to its capability to rapidly disseminate information to a broader audience without fact verification and resulting in an increase in misinformation spread throughout.[2] The rate at which the information is generated and shared could cripple any human-based fact-checking system and reliable identification of fake news.[3] Hence, it raises a compelling need for developing technologies that can fact-check and verify information posted online. Although social media companies have active algorithms to minimize misinformation based on pre-defined rules, they cannot automatically flag carefully manipulated information to deceive consumers.[2] Studies that have analyzed social media platform data related to distinct narratives like conspiracy theories and scientific news have shown that the spread of misinformation resulted in homogeneous and polarized communities.[4,5]

Among the different types of misinformation, the most commonly generated fake information is through fake audio and/or video data. The advancements in Artificial Intelligence (AI) based generative models have enabled alterations of multimedia recordings using simple user-friendly interfaces. For users without any relevant background experience, the generative software can be easily utilized to create any media content as the user prefers with little training data available.[6] As fake multimedia emerged, so did innovative detection technologies.[7,8] Using the image-level information and spatiotemporal analysis from the multimedia recordings, patterns emerged which were peculiar to fake media. The detection models were enhanced for media content analysis, but subtle changes in the parameters of uploaded content still bypass the detection.[9] The acquisition devices like cameras or audio recorders attach a wide variety of metadata information to the digital recordings capturing the information about the acquisition process.[10] Information like the source acquisition device, time, capture settings, time, and region of recording is embedded as Metadata information in each multimedia recording. Manipulation of such information could still result in falsely perceiving the information posted online.

The integration of metadata information has helped with large-scale multimedia management and passive information retrieval on the media generation origins. However, such information can easily be modified using software tools and rewriting the source properties of a media recording. The authenticity of metadata information is relevant since critical online information can be verified by fact-checking the source material like video or audio recording properties. By carefully manipulating the time or the region of recording, a perpetrator can manipulate the perception of the information posted. The current social media networks are the primary source of fake information spread through metadata manipulation since there aren't any valid verification processes of the media content.[9] Along with media content authentication, reliable measures are required to verify the media metadata information.

In this work, we focus on metadata verification of multimedia recordings using environmental fingerprints like Electrical Network Frequency (ENF) signals as a unique identifier of the source time and region of recording. ENF is the power system frequency with a nominal value of 60 Hz in the United States and 50 Hz in most European and Asian countries.[11] Due to the supply and demand variations in the power grid from the consumers of the grid, the interconnect power generator compensates by fluctuating the nominal power frequency. Thereby, random fluctuations occur in the power system frequency which varies with time and as a result is known as the ENF signal.[12] The ENF fluctuations are leveraged to authenticate digital media recordings as the media acquisition process captures the signal from its environmental presence.[13,14] For audio recordings, the ENF is captured as a result of background hum[15,16] or through the electromagnetic induction.[11,12]

In the case of video recordings, the image acquisition device captures the artificial photons from artificial light powered by the electrical grid. These artificial photons carry the ENF fluctuations in the form of illumination frequency and thereby are captured in indoor video recordings.[17,18] The ENF signal has unique, random, and unpredictable frequency fluctuations which vary with time.[19] In this paper, we built a reference database collector to collect ENF fluctuations from each power grid interconnect and verify the time and location of recording metadata information from multimedia posted to social media platforms. Due to the variance of ENF signal within the interconnect, the accuracy of the location data is verified by locating the source power grid interconnect compared to its geographical coordinates. The main contributions of this work are presented as follows,

- A novel approach to verify the timestamp and location information in audio and video recording from online social media platforms leveraging the embedded ENF signals as an environmental fingerprint.
- For media recordings without metadata information, an ENF signal based technique is proposed to estimate the source time of recording and inter-grid location data.
- A promising solution is suggested to detect forged metadata information by cross-referencing ENF signal information, and estimating original time and region of recording.
- A Decentralized ENF-based Media Authentication (DEMA) system is proposed, which encapsulates the metadata verification of media recordings in online social media using the hierarchical ENF map.
- For intra-grid location accuracy, a case study is conducted to approximate the location of media recording based on the ENF comparison to the reference database.

The rest of the paper is organized as follows. The role of metadata in modern social media platforms and the importance of ENF-based media authentication is presented in Section 2. Leveraging the ENF signals the metadata information from media recordings are validated in Section 3. A decentralized and hierarchical ENF map called the DEMA system is presented in Section 4, along with a case-study for region of recording identification. Finally, Section 5 presents our conclusion from the proposed work and discusses further steps.

## 2 Background and Related Work

### *2.1 Role of Metadata in Digital Media Publication*

The data collected from the digital acquisition device such as audio, video, and images are unstructured binary data. Hence, metadata is used as reference data to interpret the captured data. With an increase in broadcast production and online social media platform, rich metadata is becoming a key part of the multimedia production pipeline.[20] Increase in the varied consumption medium like Augmented Reality (AR) and heterogeneous platforms, media hosting services require metadata for cataloging in their vast databases and efficient retrievability. To efficiently manage and exchange multimedia information, metadata is required to standardize interoperability.[21] The emergence of various file formats has resulted in many metadata formats and variations. There is some

metadata information that cannot be altered for the life cycle of the represented data, and there are some that can be modified. Metadata can carry custom user-generated watermarks, image-related modifications like Photoshop edits, and content-related parameters like compression factors.[22]

As metadata consists of media related properties and required parameters, the origins of the generated media are also an important parameter. The time and location of creation allow users to reference their media, which is leveraged by media application developers to provide a better user experience. However, for general public information-based media like news, it is important that the provided media information can be verified based on its source.[8] As there are software technologies that are available to allow users to manipulate the media metadata to spread misinformation, it is essential now to identify such forgeries.

### *2.2 Digital Multimedia Metadata Verification*

Unaltered metadata information serves as a backbone for digital forensic analysis of multimedia. In JPEG format images, which is a compressed format, the metadata stores several parameters like the quantization tables for decompression. Thereby, it makes the JPEG file information very important for forensic evidence.[10] Image-level analysis reveals foreign frame insertions or deletions by observing the compression artifacts. Innovations in information hiding have surpassed the steganographic ways, and more information is hidden in the underlying metadata.[23] A digital certificate relating to an image file can be inserted inside that image file along with accompanying metadata containing references to the issuing company. Although metadata information carrying sensitive information like geographical location can hinder personal privacy, it is also required to be publicly available for authenticity and copyright verification. Hence, it is a double-edged sword.[9] It is very significant to secure metadata information and maintain its authenticity by preserving the attributes that are susceptible to alterations.

Social media platforms rely on the user metrics generated, and the audience is influenced by the metrics presented by the publisher. A social media user observing/researching a topic can be influenced by which source information has higher approval ratings or user engagement. By falsely manipulating the metadata information, such metrics are susceptible to forgery.[24] Traditional approaches to fake news detection in social media relied upon studying the individual user's accounts and rising content conflicts[2] Characterization of an overwhelming amount of uploads could be ineffective due to the time taken for detailed analysis.

Based on industry media standards, there are three most commonly used types of metadata, EXIF (Exchangeable Image File Format), IPTC (International Press Telecommunications Council), and XMP (Extensible Metadata Platform). The EXIF data represents the technical data carrying the acquisition processes details like device information, time, and GPS coordinates. The IPTC format is a predefined length metadata that represents the source information like the author along with the copyright, whereas the XMP allows for additional text information to be embedded. Most commonly XMP format tracks the changes made to the source file from different editing software. For our experiment, we focus on validating the information fields which are highly susceptible to forgery and changing the perception of content. Therefore, the EXIF-based metadata information like the time of creation along with the geographical location is our primary goal. Figure 1 represents the metadata of a mobile phone video recording with both time of creation and the respective GPS coordinates. For Metadata extraction from media files, we used ExifTool for our

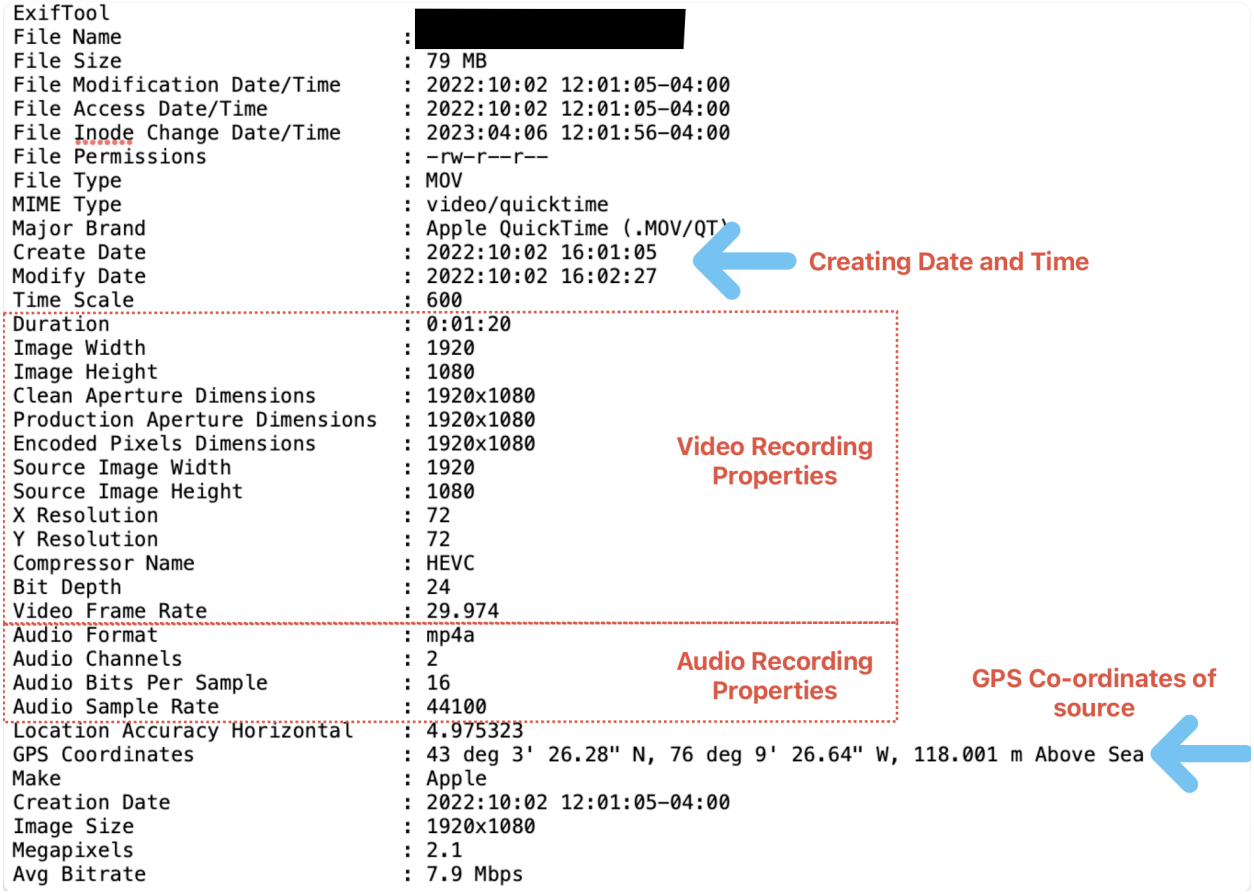



**Fig 1** Metadata of a video recording from Mobile Phone with time and region of recording data.

experiments.[25] The ExifTool can also be used to modify the metadata of the source content. The importance of protecting the source authenticity and minimizing the rapid misinformation spread has called for a reliable and effective detection technique. By leveraging environmental factors like ENF, which is not subjected to predictions or manipulations, the digital media are naturally watermarked with a unique signature.[26]

### *2.3 ENF in Multimedia Recordings*

The presence of ENF in digital audio recording was first observed in verifying the authenticity of a digital recording presented in court proceedings.[27] The manipulations made to the audio recording were detected by analyzing the changes in the phase of the signal and ENF spectrum discontinuity. For audio recordings, the process of ENF embedding in media occurs through two different mediums. The recorders directly connected to the power grid would capture ENF in the form of electromagnetic induction.[11] However, most modern audio recorders are battery-powered, so studies observed ENF patterns in battery-powered devices as a result of background hum generated from the electrical devices in the vicinity.[15,16]

The video recordings capture ENF through the photons from the illumination frequency of the artificial lights.[17] The capturing mechanism however depends on the type of imaging sensor used

in digital cameras. There are two most commonly used sensors, Complimentary Metal-oxide-semiconductor (CMOS) and Charge-coupled device (CCD). Each sensor has its unique shutter mechanism. The CCD sensor relies on a global shutter mechanism where the whole frame is activated simultaneously to capture incoming photons.[17] In CMOS sensors, a rolling shutter mechanism is used, where each row of the sensor is sequentially activated.[28] Due to the Nyquist criterion, to capture an illumination frequency of 120 Hz, a minimum sampling rate is required which is satisfied by CMOS sensors due to each row capturing individual samples. For CCD, the sampling rate is limited by the number of frames used. In terms of usability and cost-effectiveness, CMOS sensors are the most commonly used sensor in gadgets like webcams and mobile phones. From the captured samples from both audio and video, a non-parametric spectral estimation technique called as Short-Time Fourier Transform (STFT) is used to reliably estimate ENF from source recording. For further details on the estimation algorithm and frequency enhancement techniques in a noisy environment, we recommend readers to refer our previous work on ENF-based authentication systems.[14,26]

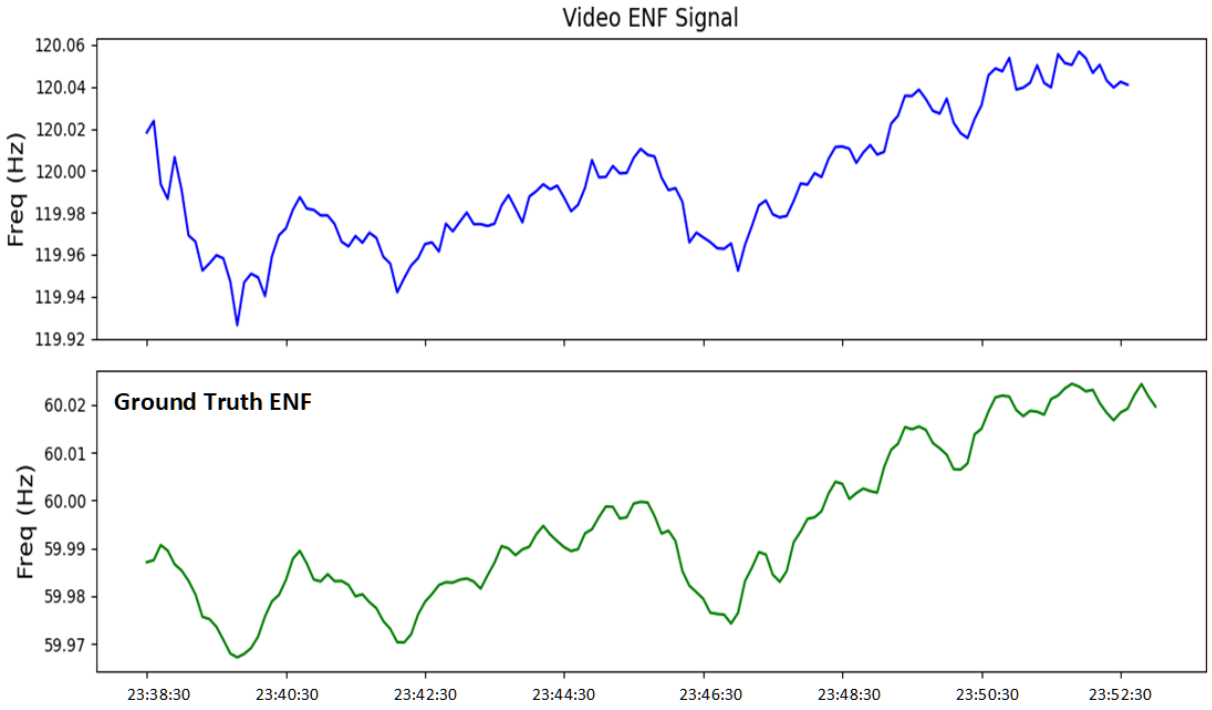
### *2.4 Environmental Fingerprint ENF Applications*

The power system frequency fluctuation caused as a result of feedback from power distribution resulted in generating a unique time-varying ENF signal. The presence of ENF in digital multimedia has enabled many forensic applications to verify the underlying media integrity. With the availability of a reference ENF signal collected from different power grid networks, ENF estimated from multimedia recordings like audio and video streams is used to verify the source time of recording[29] and the geographical location in reference to the power grid interconnect.[30] As the ENF is present in both audio and video, post-processing techniques like multimedia synchronization can benefit from ENF signal alignment from audio and video with the highest similarity correlation.[31] The continuous data collected from the Frequency Monitoring Network make use of the GPS-enabled ENF collector nodes to identify complicated power grid behaviors.[32] Leveraging the ENF signal harmonic amplitude coefficients as feature vectors, the source audio recording device can be identified[33] and the unique flicker patterns observed in captured ENF are used to identify the video recording device.[34]

The ENF signal with enough recording length can represent a unique set of fluctuations that can be used to correlate with ground truth reference data and verify the authenticity of the multimedia recording. The ENF signal estimated from both audio and video recordings can identify frame forgery attacks[14] and DeepFake attacks,[35,36] as the underlying sample changes reflect changes in fluctuation patterns. As the frequency patterns are similar throughout the grid, this feature is exploited to integrate ENF as a part of consensus protocol in a distributed computing system.[37] The ENF is estimated from participating nodes and shared through the broadcasting channel, where the nodes with faulty or manipulated ENF are then marked as a byzantine node.[7] Leveraging the ENF signal capability of source recording identification and authentication, we use ENF to verify the metadata information from selective online social media content.

## 3 ENF-based Metadata Verification

The metadata of a media recordings infers captures some key environmental factors in its properties, among them time and location data reveal the originality and source of information. Lever-




```
ExifTool
File Name                       : lecture.mp4
File Size                       : 727 MB
File Permissions                : -rw-rw-rw-
File Type                       : MP4
File Type Extension             : mp4
MIME Type                       : video/mp4
Create Date                     : 2022:01:23 23:38:30
Modify Date                     : 2022:01:23 23:38:30
Time Scale                      : 30000
Duration                        : 0:14:10
Image Width                     : 1920
Image Height                    : 1080
Video Frame Rate                : 29.998
```

**Fig 2** ENF signals from source video recording and ground truth ENF database matched based on time and duration of recording.

aging the time and location properties, the ENF is explored to provide correlation between the information gathering and its environmental factors. To integrate ENF as an authentication factor, a reference database is built to collect ENF data from different power grid interconnects. For our testbed in the United States, there are four primary power grid interconnects. The ENF collector circuits composed of step-down transformer and voltage divider circuit are deployed through the interconnect to collect ENF data with accurate time stamp and geolocation information, and store it in a database. The reference ENF provides ground truth information on the origins of a media recording. Figure 2 represents the ENF of a video recording with a nominal ENF at 120 Hz due to the illumination frequency. Using the timestamp of the video recording along with its duration, the database ENF is represented as the ground truth ENF. From inference, it is clear that the media recording has accurate time stamp information.

With the ENF database deployed in all power grid interconnects, for a source media recording where the time or location parameters are unknown but ENF is available, a distributed search across the ENF database is estimate the unknown parameters. For large-scale comparison of ENF,

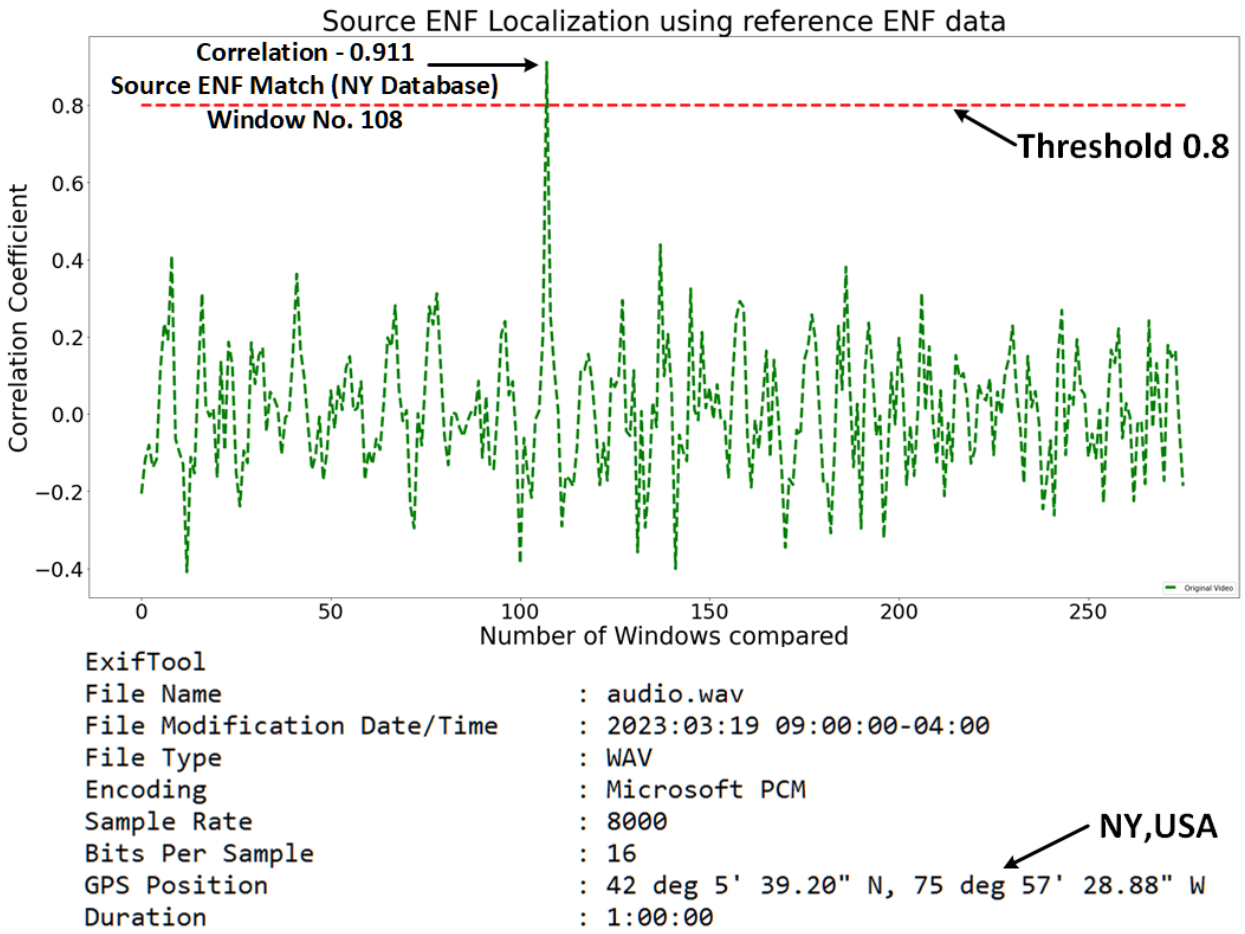



**Fig 3** Time of recording estimation of source audio recording using correlation coefficient.

a visual verification is not reliable. Therefore, we use correlation coefficient as a similarity verification factor. The correlation coefficient varies in between $1$ and $-1$, where a correlation of $1$ represents highest similarity and vice versa. From our experiments, we use a threshold of $0.8$ as a minimum viable similarity factor. In Figure 3, without inferring the metadata information, the ENF is estimated from the source audio recording and is compared against the eastern interconnect ENF database. To allow for accurate signal comparison, a sliding window approach is used.[14] Using a window of $60$ minutes and a shift of $5$ minutes, a correlation peak of $0.911$ is observed at window number $108$. Using the window number and the shift parameter, the timing of the source audio recording is concluded as 9:00 AM on March $19^{th}$. The metadata information is included in Figure 3 to verify the estimated parameters, where the GPS coordinates belong to eastern interconnect location.

In social media applications, live video streams collected in indoor environment are uploaded. Using tools like Exiftool,[25] the metadata information can be easily accessed as well as modified. In situations where the uploaded media is leveraged as an evidence to support a claim, then the media recording can be subjected to various tests. The examination include proof of authenticity which is tested in both media information forgery detection against attacks like DeepFake[7] and Metadata consistency. Using ENF-based authentication, both media content and metadata can be verified.

```
ExifTool
File Name                       : youtube_recording.mp4
File Modification Date/Time     : 2023:03:07 17:08:00-04:00
File Type                       : MP4
Image Size                      : 1920x1080
Video Frame Rate                : 29.974
GPS Position                    : 33 deg 1' 18.58" N, 96 deg 41' 57.32" W
Duration                        : 00:10:00
```

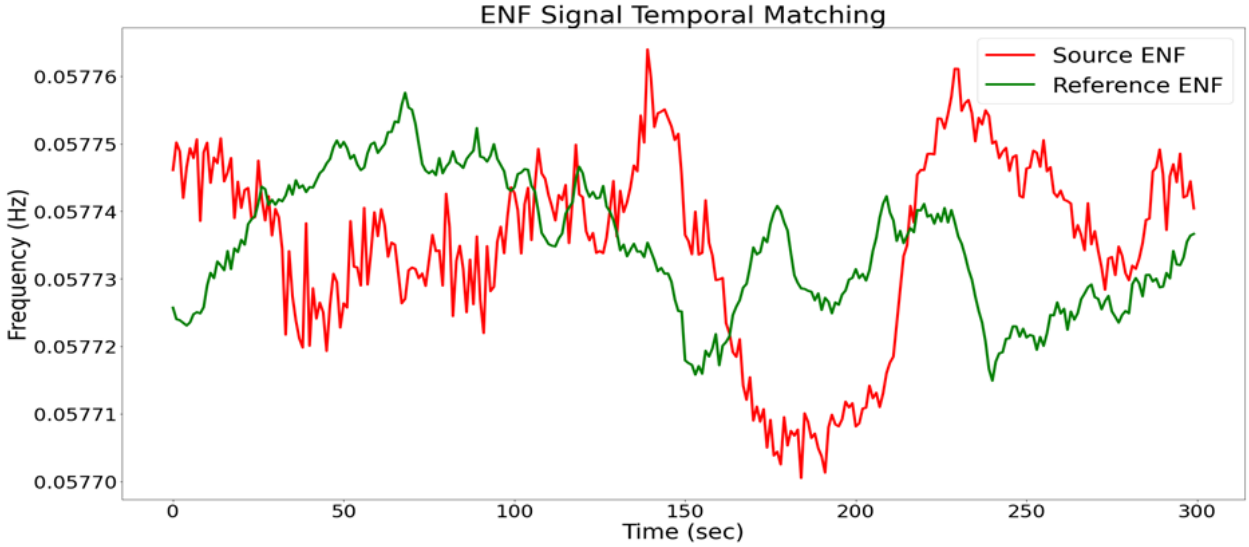



**Fig 4** Detecting modified metadata information by comparing reference ENF signal based on time-stamp and geographical location.

Using the Exiftool, we modified the GPS and date-time metadata information of a youtube recording made in an indoor environment. By cross referencing the ENF recording from its respective database, the mismatch in ENF signal can be observed in Figure 4. The nominal frequency of the video recording is $120$ Hz and the ground truth power recording is $60$ Hz. For visual comparison, both the ENF signals are normalized in Figure 4. The signal correlation coefficient is $0.38$ which is below the threshold value, and therefore the metadata information from the source recording is concluded as tampered or modified. Along with fake metadata detection, the estimated source ENF recording can be used to estimate the origins of the recording by investigating all ENF databases.

Using the modified Youtube recording, the source ENF is cross referenced across all the ENF database in all interconnects, since the location is assumed unknown. Using the sliding window approach, source ENF is compared with the reference ENF signal from available databases at the same time using vector operation to minimize the compute time. In Figure 5, an ENF match is identified on March $17^{th}$ at $5:05:00$ AM from the ENF database in New York (Eastern Interconnect). The respective correlation coefficient is $0.97$ for the ENF match, and it can be seen that there is a single correlation coefficient greater than the threshold. From the source time and location identification of an unknown recording using the metadata information, the ENF-based verification has reliably supported in minimizing the misinformation associated with metadata forgery. It is clear that the metadata verification is dependent on the authenticity of reference ENF signal, so protecting the ENF database from external forgery is a high priority.

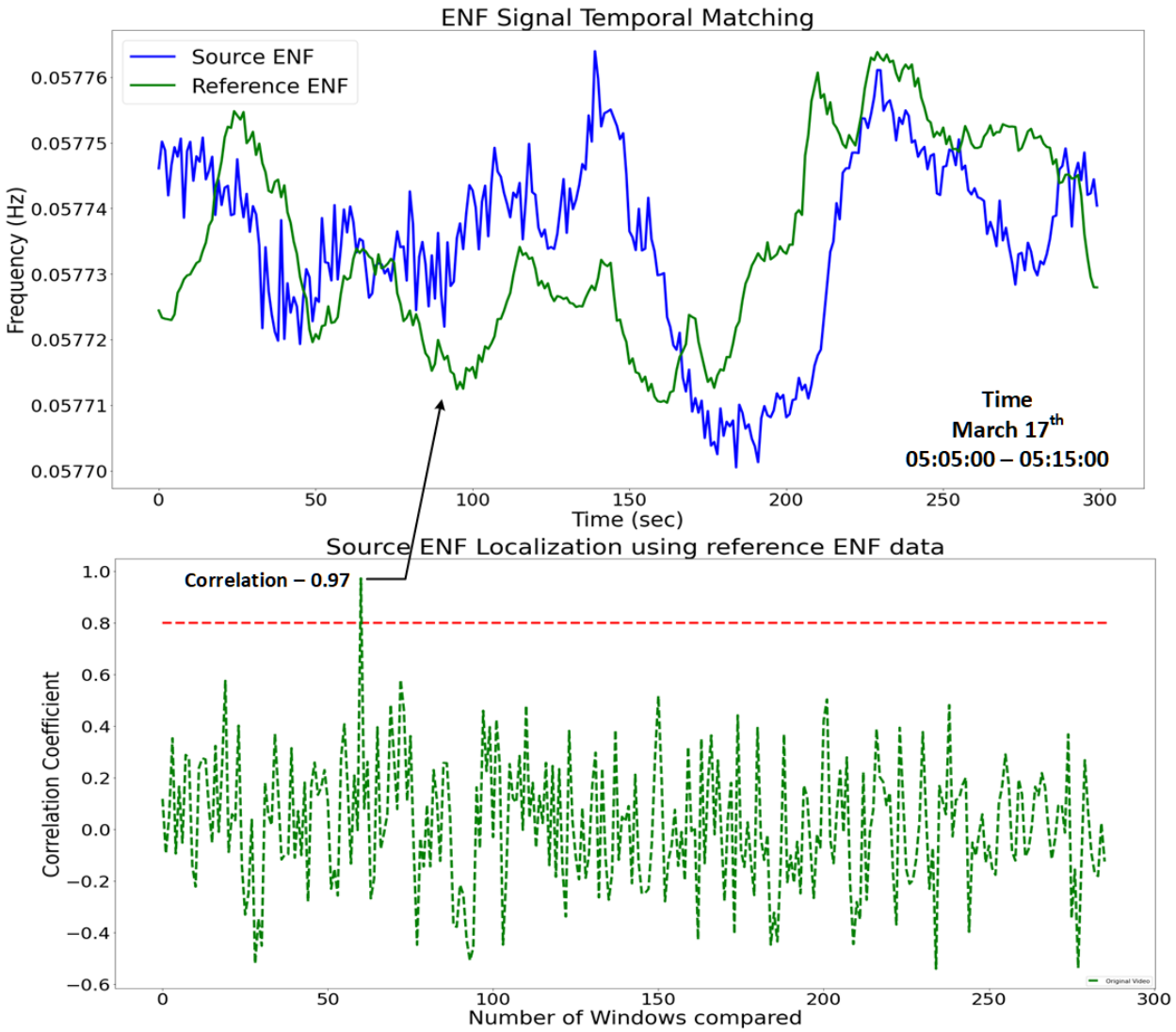



**Fig 5** Source Time and Location identification using media ENF signal and reference database.

Leveraging the ENF verification process, we propose a Distributed ENF-based Media Authentication (DEMA) system to construct a hybrid distributed system consisting of both decentralized ENF capturing nodes capable of self-authenticating[37] and a hierarchical architecture to allow for intra-grid localization. The following section will discuss our proposed system design, and allow users to verify the authenticity of media recording by integrating the DEMA framework as an API request.

## 4 DEMA System

The DEMA leverages Blockchain technology and hierarchical edge-fog-cloud computing paradigm to provide a secure-by-design and trust infrastructure for metadata verification of media recordings in online social media. Figure 6 demonstrates an overview of DEMA system architecture in which the left part shows a states-level grids map of US that consists of five regional power networks. Each regional power grid has a dedicated server to manage ENF data within the network. All five

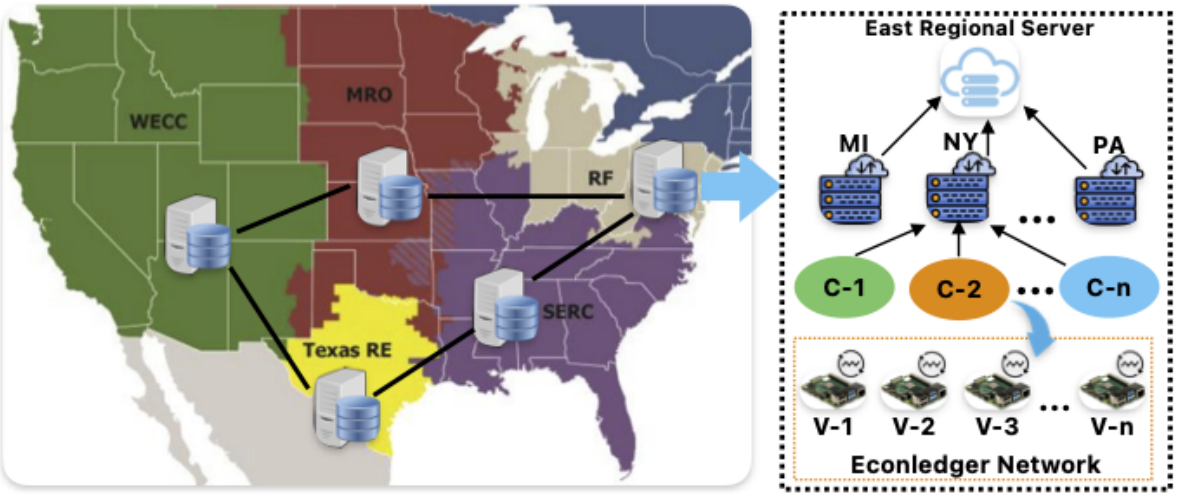



**Fig 6** DEMA System Architecture.

regional servers relies on security communication channels to share data. Figure 6 shows that the region power networks Midwest Reliability (MRO), ReliabilityFirst (RF) and SERC Reliability are part of the Eastern Interconnect, and thereby consists of similar ENF fluctuations with minor difference due to the propagation delays.[38]

The right part of Figure 6 represents the hierarchy of federated data aggregation within a RF regional grid network, which consists of the cloud, fog and edge computing layers. The edge computing layers are deployed at multiple fragmented cities. Each city relies on a permissioned blockchain network that can provide public key infrastructure, identity authentication, access control, and resources management. In a city, a set of registered edge devices $V \in [V_1, V_2, ..., V_n]$ are geographically scattered and they connect the same grid network. Each edge device $V_i$ extract environmental fingerprint information, like multimedia metadata and time serial ENF vectors.

To guarantee security, availability and resilience under a distributed edge network environment, the Econledger fabric[37] is adopted to provide decentralized and secure data storage and sharing services at the city level. Econledger uses a distributed database (DDB) to distributively store multimedia records along with environmental fingerprint data rather than a centralized server. In addition, Econledger allows edge devices to cooperatively execute a lightweight PoENF consensus protocol to make agreement on the ground truth ENF and metadata that are stored on a tamper-proof and verifiable distributed ledger without relying on any third party authority. Thanks to Econledger, each city can maintain a trustworthy database containing the city level environmental fingerprint data, which provide a solid foundation for the federated data aggregation.

Inspired by ideas of a hierarchical federated learning framework,[39] DEMA uses a federated data aggregation scheme to construct a regional database from the bottom to the up, as Figure 6 shows. At the fog level, each state has a trust server that collects data from cities and performs data aggregation algorithms. For example, New York state periodically collect a set of its city databases that is represents as $C_i \in [C_1, C_2, ..., C_n]$. Then it performs data averaging to get state database represented as $S_{NY} = \frac{1}{n}\sum_1^n(C_i)$. Other states follow the same procedures to calculate their state database. Finally, the east regional server deployed on the cloud level collect databases from multiple states and then perform averaging to construct the regional database $RF$.

The DEMA system allows for hierarchical search of time and location based analytics given

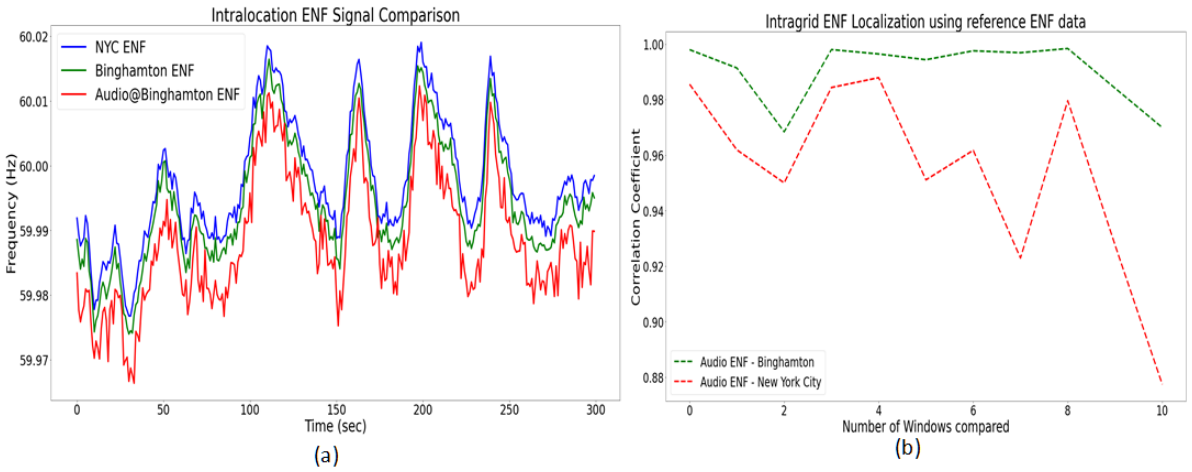



**Fig 7** (a) ENF from Audio recording at Binghamton City, along with reference ENF data from Binghamton and NYC database; (b) Intra-grid Localization of Source ENF recording by comparing correlation coefficient similarity.

an unknown source recording. The accuracy of the overall aggregation improves when the ENF collection nodes are deployed at more granular scale.[32] The time of the source recording can be identified using the Regional server aggregated ENF signal, however, the location of the recording varies from one region of the grid to other due to the propagation delay.[40] Given the time of the recording is synchronized from an unknown recording, we present a case study on region of recording identification using the local ENF database nodes. The Figure 7(a) represents the ENF signals collected from an audio recording in the Binghamton city region from Eastern interconnect. Along with the audio recordings, the ground truth ENF signal from local Binghamton database along with the New York City (NYC) database which are approximately 200 miles apart is presented in Figure 7(a). Although the signals carry very similar fluctuations, the propagation delay introduces minor variations to the signal. The ENF signals are compared using the correlation coefficient along with the sliding window protocol. From Figure 7(b), the correlation coefficient between the audio and Binghamton node along with audio and NYC server is presented. Compared to the previous experiment, both the correlations are above the threshold, but the signal similarity varies on a granular scale. It is clear that the correlation between the Audio ENF and the Binghamton node is higher compared to the NYC node, and thereby concludes that the audio was recorded near the Binghamton region. By integrating more ENF nodes throughout the interconnects, the region of recording identification can be more localized to the city-level.

## 5 Discussion and Conclusions

With growing social media network capabilities and information shared over the network, misinformation spread has become an increasing threat to the community. Advancements in authentication techniques have prioritized media content analysis for integrity verification, however, the perception of the media could still be susceptible to subtle changes made to the metadata information. In this work, we introduce an ENF-based metadata verification system for time and location of source recording estimation. From our experiments, for online media recordings with modified metadata information, the reference ENF from the regional database can be leveraged to verify the origin of recording data. In the case of media recordings with unknown time and location parameters,

the source ENF is correlated with the ENF database collections using a sliding window approach and estimates the unknown parameters. A hybrid distributed network DEMA is proposed by leveraging the federated data aggregation scheme to construct a regional ENF database from remotely deployed ENF collection nodes. For secure media verification, it is evident that the ground truth information provided by the DEMA system remains protected against external forgery attacks. The PoENF lightweight consensus protocol enables faulty node detection along with mutually agreed ground truth data among the participating nodes.

In generic media networks, privacy concerns are currently a leading concern for participating users. A GPS-leakage by an image published online by an unaware social media user resulted in an incident on Apache choppers.[41] However, the purpose of the proposed system is to verify the information published online claiming to be evidence of critical news. Metadata information could be a double-edged sword, and public access to such information could be a privacy concern. The results from ENF-based location estimation are however not extremely granular, the location inference from the ENF is subjected to the power grid where the recording was made. So, using the proposed system, the users can still preserve their privacy on a granular level.

ENF estimation from various formats of media recordings could also include recordings with a lower signal-to-noise ratio, where the ENF harmonics are affected by external noise. The proposed system leverages edge-fog-cloud architecture, so the DEMA system can be integrated with additional signal enhancement algorithms to minimize the noise and improve the ENF signal. The cloud layer provides additional computational resources for advanced algorithms, so the ENF reference database nodes remain unaffected by noisy input. Integrating additional ENF collection nodes can help with region of recording identification compared to the grid-level identification. To support the battle against misinformation, we plan to further improve the proposed architecture as a service for users to verify both the content level and metadata analysis given the source URL of the media recordings.

*References*


1 G. D. Domenico, J. Sit, A. Ishizaka, *et al.*, "Fake news, social media and marketing: A systematic review," *Journal of Business Research* **124**, 329–341 (2021).

2 K. Shu, A. Sliva, S. Wang, *et al.*, "Fake News Detection on Social Media: A Data Mining Perspective," *ACM SIGKDD Explorations Newsletter* **19**, 22–36 (2017).

3 S. Bhatt, N. Goenka, S. Kalra, *et al.*, "Fake News Detection: Experiments and Approaches Beyond Linguistic Features," in *Data Management, Analytics and Innovation*, N. Sharma, A. Chakrabarti, V. E. Balas, *et al.*, Eds., *Lecture Notes on Data Engineering and Communications Technologies*, 113–128, Springer, (Singapore) (2022).

4 M. Del Vicario, A. Bessi, F. Zollo, *et al.*, "The spreading of misinformation online," *Proceedings of the National Academy of Sciences* **113**, 554–559 (2016). Publisher: Proceedings of the National Academy of Sciences.

5 D. Acemoglu, A. Ozdaglar, and A. ParandehGheibi, "Spread of (mis)information in social networks," *MIT web domain* (2010). Accepted: 2011-03-18T21:06:59Z Publisher: Elsevier B.V.

6 I. Perov, D. Gao, N. Chervoniy, *et al.*, "DeepFaceLab: Integrated, flexible and extensible face-swapping framework," *arXiv:2005.05535 [cs, eess]* (2021). arXiv: 2005.05535.

7 D. Nagothu, R. Xu, Y. Chen, *et al.*, "DeFakePro: Decentralized Deepfake Attacks Detection Using ENF Authentication," *IT Professional* **24**, 46–52 (2022). Conference Name: IT Professional.

8 H. Choi and Y. Ko, "Effective fake news video detection using domain knowledge and multimodal data fusion on youtube," *Pattern Recognition Letters* **154**, 44–52 (2022).

9 M. Shaliyar and K. Mustafa, "Metadata Analysis of Web Images for Source Authentication in Online Social Media," in *Mathematics and Computing*, B. Rushi Kumar, S. Ponnusamy, D. Giri, *et al.*, Eds., *Springer Proceedings in Mathematics & Statistics*, 75–88, Springer Nature, (Singapore) (2022).

10 T. Gloe, M. Kirchner, and C. Riess, "How we learned to stop worrying about content and love the metadata," *IFS-TC Image Forensics Challenge Special Session during WIFS* (2013). Publisher: Citeseer.

11 C. Grigoras, "Digital audio recording analysis–the electric network frequency criterion," *Int. J. Speech Lang. Law* **12**(1), 63–76 (2005).

12 A. J. Cooper, "The Electric Network Frequency (ENF) as an Aid to Authenticating Forensic Digital Audio Recordings – an Automated Approach," Audio Engineering Society (2008).

13 D. Nagothu, Y. Y. Chen, E. Blasch, *et al.*, "Detecting malicious false frame injection attacks on surveillance systems at the edge using electrical network frequency signals," *Sensors (Basel).* **19**(11), 1–19 (2019).

14 D. Nagothu, Y. Chen, A. Aved, *et al.*, "Authenticating Video Feeds using Electric Network Frequency Estimation at the Edge," *EAI Endorsed Transactions on Security and Safety* **"7"** (2021).

15 N. Fechner and M. Kirchner, "The humming hum: Background noise as a carrier of ENF artifacts in mobile device audio recordings," in *IT secur. Incid. Manag. IT forensics (IMF), 2014 eighth int. Conf.*, 3–13 (2014). tex.organization: IEEE.

16 J. Chai, F. Liu, Z. Yuan, *et al.*, "Source of ENF in battery-powered digital recordings," in *Audio eng. Soc. Conv. 135*, (2013). tex.organization: Audio Engineering Society.

17 R. Garg, A. L. Varna, A. Hajj-Ahmad, *et al.*, ""Seeing" ENF: power-signature-based timestamp for digital multimedia via optical sensing and signal processing," *IEEE Transactions on Information Forensics and Security* **8**(9), 1417–1432 (2013). Publisher: IEEE.

18 A. Hajj-Ahmad, C.-W. Wong, S. Gambino, *et al.*, "Factors Affecting ENF Capture in Audio," *IEEE Transactions on Information Forensics and Security* **14**, 277–288 (2019). Conference Name: IEEE Transactions on Information Forensics and Security.

19 N. Poredi, D. Nagothu, Y. Chen, *et al.*, "Robustness of Electrical Network Frequency Signals as a Fingerprint for Digital Media Authentication," in *2022 IEEE 24th International Workshop on Multimedia Signal Processing (MMSP)*, 1–6 (2022). ISSN: 2473-3628.

20 G. Wilkinson, T. Bartindale, T. Nappey, *et al.*, "Media of Things: Supporting the Production of Metadata Rich Media Through IoT Sensing," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, *CHI '18*, 1–13, Association for Computing Machinery, (New York, NY, USA) (2018).

21 F. Pereira, A. Vetro, and T. Sikora, "Multimedia Retrieval and Delivery: Essential Metadata Challenges and Standards," *Proceedings of the IEEE* **96**, 721–744 (2008). Conference Name: Proceedings of the IEEE.

22 R. G. Mani, R. Parthasarathy, S. Eswaran, *et al.*, "A Survey on Digital Image Forensics: Metadata and Image forgeries," (2022).

23 M. Harran, W. Farrelly, and K. Curran, "A method for verifying integrity & authenticating digital media," *Applied Computing and Informatics* **14**, 145–158 (2018).

24 D. Kuchhal and F. Li, "A View into YouTube View Fraud," in *Proceedings of the ACM Web Conference 2022*, *WWW '22*, 555–563, Association for Computing Machinery, (New York, NY, USA) (2022).

25 "ExifTool by Phil Harvey."

26 D. Nagothu, R. Xu, Y. Chen, *et al.*, "Deterring Deepfake Attacks with an Electrical Network Frequency Fingerprints Approach," *Future Internet* **14**, 125 (2022). Number: 5 Publisher: Multidisciplinary Digital Publishing Institute.

27 C. Grigoras, "Applications of ENF criterion in forensic audio, video, computer and telecommunication analysis," *Forensic Science International* **167**(2-3), 136–145 (2007). Publisher: Elsevier.

28 H. Su, A. Hajj-Ahmad, R. Garg, *et al.*, "Exploiting rolling shutter for ENF signal extraction from video," in *Image process. (ICIP), 2014 IEEE int. Conf.*, 5367–5371 (2014). tex.organization: Citeseer.

29 G. Hua, Q. Wang, D. Ye, *et al.*, "Reliability of Power System Frequency on Times-Stamping Digital Recordings," *arXiv:2011.00176 [cs]* (2020). arXiv: 2011.00176.

30 D. Chowdhury and M. Sarkar, "Location Forensics Analysis Using ENF Sequences Extracted from Power and Audio Recordings," *arXiv:1912.09428 [cs, eess, stat]* (2019). arXiv: 1912.09428.

31 K. Vidyamol, E. George, and J. P. Jo, "Exploring electric network frequency for joint audio-visual synchronization and multimedia authentication," in *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, 240–246 (2017).

32 Y. Liu, S. You, W. Yao, *et al.*, "A Distribution Level Wide Area Monitoring System for the Electric Power Grid–FNET/GridEye," *IEEE Access* **5**, 2329–2338 (2017). Conference Name: IEEE Access.

33 D. Bykhovsky, "Recording device identification by ENF harmonics power analysis," *Forensic Science International* **307**, 110100 (2020).

34 A. Hajj-Ahmad, S. Baudry, B. Chupeau, *et al.*, "Flicker forensics for pirate device identification," in *Proc. 3rd ACM work. Inf. Hiding multimed. Secur.*, 75–84 (2015). tex.organization: ACM.

35 D. Nagothu, R. Xu, Y. Chen, *et al.*, "DeFake: Decentralized ENF-Consensus Based DeepFake Detection in Video Conferencing," in *IEEE 23rd International Workshop on Multimedia Signal Processing*, (Tampere, Finland) (2021).

36 D. Nagothu, R. Xu, Y. Chen, *et al.*, "Detecting Compromised Edge Smart Cameras using Lightweight Environmental Fingerprint Consensus," in *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, *SenSys '21*, 505–510, Association for Computing Machinery, (New York, NY, USA) (2021).

37 R. Xu, D. Nagothu, and Y. Chen, "EconLedger: A Proof-of-ENF Consensus Based Lightweight Distributed Ledger for IoVT Networks," *Future Internet* **13**, 248 (2021). Number: 10 Publisher: Multidisciplinary Digital Publishing Institute.

38 C.-W. Wong, A. Hajj-Ahmad, and M. Wu, "Invisible Geo-Location Signature in A Single Image," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 1987–1991 (2018). ISSN: 2379-190X.

39 R. Xu and Y. Chen, "$\mu$dfl: A secure microchained decentralized federated learning fabric atop iot networks," *IEEE Transactions on Network and Service Management* **19**(3), 2677–2688 (2022).

40 R. Garg, A. Hajj-Ahmad, and M. Wu, "Feasibility Study on Intra-Grid Location Estimation Using Power ENF Signals," *arXiv:2105.00668 [eess]* (2021). arXiv: 2105.00668.

41 R. Bhangale, "Securing Image Metadata using Advanced Encryption Standard," Master's thesis, Dublin, National College of Ireland (2020).