B20 Determination of Time of Recording With Electric Network Frequency (ENF)

Maarten Huijbrechtse, BS, and Zeno J. Geradts, PhD, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS*

After attending this presentation, attendees will gain knowledge of how Electric Network Frequency assists in determining the authenticity of a recording, tampering, the time of recording utilizing ENF, how to collect ENF, and validation of results with statistical background.

This presentation will impact the forensic community by giving an overview of the current status of ENF-research, tests to validate the results, and to use a Bayesian approach for conclusions.

In casework, sometimes there are doubts regarding the authenticity of a recording. Has a crime been committed at a certain time, when for example someone recorded it with a video camera on a phone? There can be time stamps on the recording; however, sometimes there is also the signal of the electricity network available on the recording.

The European network has 50 Hz as mail frequency, whereas the U.S. network has 60 Hz. However, it is known from various research studies, for example by Grigoras, that over time, the frequency is not constant, but fluctuates around 50 Hz in a presumably random way. At each point in time, the fluctuation is the same throughout the entire network.

It is also known that a digital audio recording can contain the ENF signal if it has been recorded with mains powered equipment (Grigoras). Further, according to Kajstura et al., it is possible to detect the ENF signal in a recording made with battery-powered equipment.

Grigoras and Kajstura et al. have shown that it is possible to verify or falsify a questioned time of recording by comparing the ENF signal from the recording with a database of the ENF fluctuation. The natural follow-up question is: Can we use the ENF signal from a digital audio recording to determine its (unknown) time of recording? Our research aims at answering this question.

A database was created of the ENF fluctuation that was recorded from September 2005 to February, 2007 (with some interruptions). This database is reported to differ less than 2 mHz from frequency measurements by the Swiss ETRANS company.

This database is used to test the randomness of the ENF fluctuation. This was completed by computing typical correlation coefficients (*r*) and root-mean-squared differences (*e*) for two separate pieces of equal length from the database. With *r* close to 1 and *e* close to 0, the pieces are determined to be (almost) identical. Ideally, this only happens when the two pieces are in fact not separate ones, but the same ones.

Furthermore, ENF fluctuation were collected for a month. During this collection process, several audio recordings were made both in uncompressed (.WAV) and compressed (.MP3) format. By matching the ENF signal from these recordings with the collected ENF fluctuation, testing to determine whether *r* and *e* are significantly closer to 1 and 0 respectively than the typical values found from the database was conducted, and thus whether a recording can be uniquely positioned in time.

Future research could be aimed at determining with which network a certain recording has been made. The difference for example between the American network (60 Hz) and the European network (50 Hz) might be obvious. A recording can also be made with a generator, which could also have certain ENF patterns. Future research within this field could also include checking for patterns derived from ENF for example in the images of video streams or other sources.

For forensic research it would be necessary to have ENF databases from electricity networks that are not connected and accessible to other forensic scientists. A java applet for acquisition has been developed for the acquisition. A challenge is to have a reliable signal from the different networks in the world, in which different laboratories in the world can acquire data from the different networks. When large ENF databases from different networks are available, it is possible to compare the databases, which helps in determining authenticity of a recording in forensic science. Also in the forensic conclusion of the report it becomes possible to conclude in a Bayesian approach, since statistics are available from these database, and conclusions drawn are more objective.

ENF, Electric Network Frequency, Audio