Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-16-09

How to Apply **Create and release your Profile on Zintellect** – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 2 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

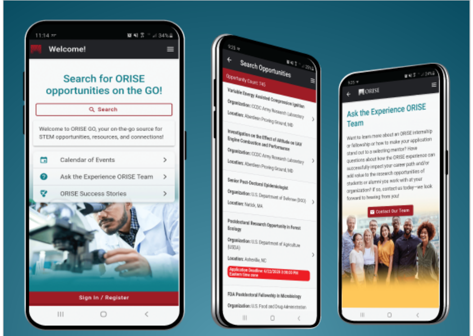
Application Deadline 4/15/2016 6:00:00 PM Eastern Time Zone

Description Importance of Authentication

Digital multimedia may be subject to accidental or deliberate modification, including tampering. The authentication process determines whether or not the multimedia recording in question has been modified. In the past, analog recordings were authenticated with processes akin to examining a bullet and the barrel it was shot from in that examiners looked for mechanical splices or overdubbing signatures in a physical master analog tape. In this age of digital multimedia, edits can be made and covered up very easily. There are free versions of editing software – such as Premiere, Audacity, and Hand-Brake, which are available online and can be used to make edits that alter the events or conversation that originally occurred in digital recordings.

Within the forensic and intelligence communities there is an increasingly large amount of multimedia data (meaning both video and audio) which has undergone various forms of trans-coding, whether it be: via internet transmission; moving from a proprietary format to an open one; uploading a file to a hosting site; using social media to post; uploading a multimedia file off of a phone; or intentional alteration/editing of files to change their meaning. If digital multimedia evidence is found to be altered, it could be ruled inadmissible in court because it is not an accurate representation of the events that occurred. Further if a decision regarding National Security must be based on the multimedia data, then those making the decision – and the community at large - must be aware of what the recording actually represents, or may not represent.

The community at large is seeking a solution to verify the content of multimedia files to better understand what is being portrayed.


Welcome!
Search for ORISE opportunities on the GO!
Search
Calendar of Events
Ask the Experience ORISE Team
ORISE Success Stories
Sign In / Register
Search Opportunities
Ask the Experience ORISE Team

Such solutions are not only needed to examine individual files on a case-by-case basis, but also to perform automated analysis of large volumes of digital multimedia files in order to perform triage so that files may be subdivided into categories for further analysis, depending upon whether the automated techniques indicate modification or a lack thereof.

Example Approaches

Current approaches to digital multimedia file authentication rely heavily upon manual examination of the content and the digital file properties. These manual processes include the following: Use of a HEX editor to identify evidence of editing; Analysis of metadata to determine if there are any signatures associated with tampering or a lack of signatures expected in authentic files; the use of PRNU (Photo-Response-Non-Uniformity – i.e., noise signatures of the photos or videos); finding a control signal from an audio recording device; examining files for double compression (i.e. finding regions that appear to have been altered or audio components that emit a different noise signature); examine encoding characteristics, such as quantization tables, to verify the source of the recording throughout the entire recording. Likewise, for every type of multimedia, expert analysts can also perform time-consuming manual reviews of the content in order to detect irregularities associated with tampering.

Likewise, although automated techniques to detect double compression and some metadata signatures across large volumes of multimedia have been developed for some classes of digital multimedia files (i.e., digital photographs), for the most part, the community lacks automated tools to apply to the widest variety of digital multimedia file types.

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Business** (11 👁)
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (6 👁)
  - **Computer, Information, and Data Sciences** (16 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (10 👁)
  - **Other Non-Science & Engineering** (13 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (28 👁)