

Opportunity Title: Methods to detect manipulated facial images in identity documents or on-line applications

Opportunity Reference Code: IC-18-33

Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-18-33

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.

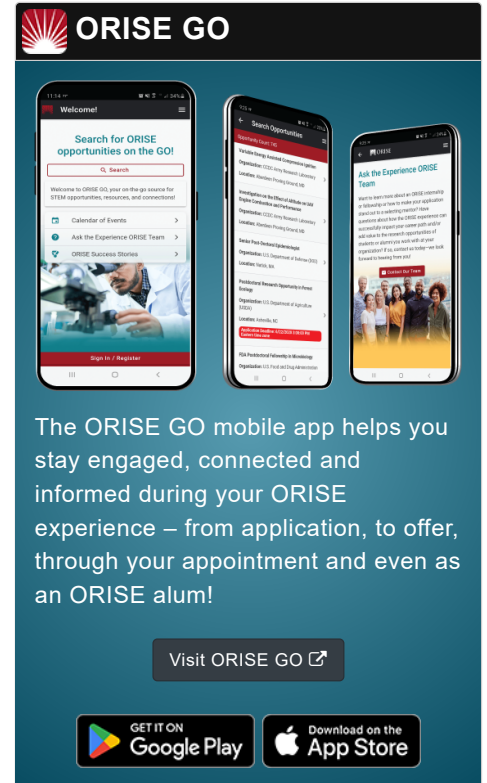
Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: <https://orau.org/icpostdoc/>.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline 3/12/2018 11:59:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

- Facial images are widely used as a primary means of establishing / verifying identity, be it in passports, drivers' licenses or staff workplace passes. Automated facial recognition technology is increasingly being used to automate the identity verification process and to confirm that the image printed on the document or stored in the chip is of the person presenting it.
- It has recently become clear that such systems have a vulnerability if the application and enrolment process provides an opportunity for the applicant to digitally modify the image prior to submission. This may be for benign reasons (e.g. to make their face look more attractive) or it may be done for more malicious reasons, for example to defeat a duplicate check during the application process, thereby allowing an individual to obtain multiple identity documents under different names. Another possibility is that images of two or more individuals may be digitally combined (morphed) to create an image and thus obtain an identity document that multiple people can then make use of. The software to do this is freely available on the web.
- Automation is increasingly being used to read identity

ORISE GO

The ORISE GO mobile app helps you stay engaged, connected and informed during your ORISE experience – from application, to offer, through your appointment and even as an ORISE alum!

Visit ORISE GO

GET IT ON Google Play | Download on the App Store

Opportunity Title: Methods to detect manipulated facial images in identity documents or on-line applications

Opportunity Reference Code: IC-18-33

documents such as passports and verify the authenticity of the document and identity of the owner, and the result of this is that there is a corresponding reduction in manual examination. However, not only can such manipulated images be used to subvert automated facial recognition systems, they are also very difficult for human examiners to detect.

- It is therefore important to research techniques which can be used for the accurate and reliable detection of manipulated images. Research should address content, but it is also possible to detect manipulated images on the basis of image meta-data.

Example Approaches:

- There are numerous tools already available in the field of image forensics designed to detect manipulated images, however none of them are currently able to reliably detect morphed images, especially in cases where the manipulated image is printed out and then rescanned, thereby removing many of the artefacts which might have been present. These typically look at compression artifacts, noise patterns, copy and paste artefacts, color filter array interpolation and local color changes etc.
- Local Binary Pattern analysis and use of Machine Learning are among newer methods that have been proposed to detect morphed images, but in all cases the lack of suitable training data is a challenge, as is that fact that there are multiple different ways in which an image may be altered.

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the application deadline
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program.

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens





Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.

Opportunity Title: Methods to detect manipulated facial images in identity documents or on-line applications

Opportunity Reference Code: IC-18-33

- **Discipline(s):**

- **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** (5 )
- **Physics** (16 )
- **Science & Engineering-related** (1 )
- **Social and Behavioral Sciences** (28 )