

## **Keynote Speech Topic:**

Image Authentication and Tamper Localization based on Semi-Fragile Hash Value

### **Abstract:**

Image authentication can be used in many fields, including e-government, e-commerce, national security, news pictures, court evidence, medical image, engineering design, and so on. Since some content-preserving manipulations, such as JPEG compression, contrast enhancement, and brightness adjustment, are often acceptable—or even desired—in practical application, an authentication method needs to be able to distinguish them from malicious tampering, such as removal, addition, and modification of objects. Therefore, the traditional hash-based authentication is not suitable for the application. As for the semi-fragile watermarking technique, it meets the requirements of the above application at the expense of severely damaging image fidelity. In this talk, we propose a hybrid authentication technique based on what we call fragile hash value. The technique can blindly detect and localize malicious tampering, while maintaining reasonable tolerance to conventional content-preserving manipulations. The hash value is derived from the relative difference between each pair of the selected DCT AC coefficient in a central block and its counterpart which is estimated by the DC values of the center block and its adjacent blocks. In order to maintain the relative difference relationship when the image undergoes legitimate processing, we make a pre-compensation for the AC coefficients. Experimental results show that our technique is superior to semi-fragile techniques, especially in image fidelity, tolerance range of legitimate processing, and/or the ability to detect and localize the tampered area. Due to its low computational cost, our algorithm can be used in real-time image or video frame authentication. In addition, this kind of proposed techniques can be extended to use other characteristic data, such as high-level moment, statistical data of image, and so on.