## J5 A Technique for Authentication of Digitally Recorded Information

*William B. Campbell, PhD*, Thomas P. Wood, BS, MSEE, MBA, Zachariah Gibson, MS, and Chadwick Cox, BS, Accurate Automation Corporation, 7001 Shallowford Road, Chattanooga, TN 37421*

After attending this presentation, attendees will be given a detailed description of a technique that enables the use of digitally recorded information as evidence.

This presentation will impact the forensic community and/or humanity by demonstrating a technique which will reduce the reluctance of organizations to use digital recordings, such as digital images, where that information may become legal evidence.

Digitally recorded information, such as an image, can be easily altered, and therefore may be difficult to offer or accept as legal evidence. A technique has been developed whereby digital recordings can be offered and accepted as legal evidence without concern of alterations. The most difficult rule of evidence for digital recordings to meet is authentication. Authentication is the means to prove, first, the conditions under which the recording was made, and, second, that the recording is offered in its original, unaltered form. The conditions under which the record was made may include date, time, location, people present, and other relevant conditions. This technique adds information to a digital recording that includes the context in which the recording was made and also includes an encrypted digital signature of the recording and context information. The authentication encode function may be integrated with the device capturing the digital information, such as a surveillance camera. This is an example of a “tightly coupled” authentication process. Alternatively, the authentication encode function may reside on a data server and add the authentication information when the records reach their final storage destination. This is an example of a “loosely coupled” authentication process. This technique produces authenticated digital records that permit unrestricted usage. Recordings such as authenticated digital images may be used with standard commercial image viewing and editing software utilities. But at any time, an authenticated digital recording may be tested to see if it has been altered. Any alteration of the recording or the context information will be definitively detected. The use of strong public key encryption processes permits widespread distribution of the public key encode process and controlled usage of the private key decode process with maximum security. Further, strong digital signature techniques based on large random numbers ensures near-certainty that any modification will be detected. This authentication technique does not alter the original recorded information in any way, as compared to techniques such as digital watermarks that alter the original data in a way that is supposedly imperceptible. This technique for the authentication of digitally recorded information may be applied to any digital information such as still images, audio recordings, full motion images, and service records. It has been implemented for standard recording formats such as JPEG, TIFF, MPEG, and WAV. It can be implemented in proprietary formats and databases for such records as maintenance or service information, telephone usage and billing records, and human resources records. Forensic science has focused great attention on “questioned documents” where most documents traditionally originated on paper. Business practices have transitioned to a point where many documents originate as digital information. This patent-pending authentication technique addresses the forensics of “questioned digital documents.”

**Authentication, Digital Recording, Evidence**

* *Presenting Author*