Brothers Technology™

Email: info@brotherstechnology.com
Phone: (203) 589-6769

The Event Verification System

(U.S. Patent No. 5,799,083)

Scenario 1: A high ranking U.S. military officer with critical knowledge of U.S. nuclear defenses has been taken hostage by a terrorist organization. They have held him for two weeks. Offering the President and his advisors a video tape, they claim he is alive and well and make their ransom demands. The advisors, however, have reason to believe the officer may no longer be alive. If he is alive, do they risk moving against the group? How do they know when the video was actually recorded?

Scenario 2: In court, a surveillance video purports to show the suspect in the vicinity of a crime at the time it was committed. The accused maintains that he is innocent. Although the recording shows someone resembling the accused, it is possible that it is, indeed, only a resemblance and that the video was not even recorded at the time or place claimed. It is even possible that the video was recorded at the purported time and place but was subsequently altered to include a likeness of the accused. How can the court ascertain the time, place, and authenticity of the recording?

Scenario 3: U.S. satellite intelligence photos show weapons being transported from Pakistan to guerrilla camps in Afghanistan. The Pakistani Government dismisses the photos as fakes. How can the international community know unequivocally when and where the photos where taken and that they were not tampered with?

Until now, under such circumstances, there have been no reliable means for addressing these difficult questions. The Event Verification System™ (EVS) offers an effective solution to the problem of video authentication. Using encryption technology, EVS prevents fraud by insuring the accurate and unalterable electronic recording of an event. Indeed, it provides a tamper-proof means for establishing the authenticity, time, and place of a digital recording along with a means for communicating this information to a safe, remote location.

While EVS can be used to keep information secret, it uses encryption primarily to protect data from alteration and certify its authenticity. Figure 1 shows a block diagram of a public key-based Event Verification System. Public key encryption algorithms are dual key encryption techniques wherein one key is used to encrypt information and the other key is used to decrypt the same information. The "private" key is kept secret by the owner while the "public" key can be freely distributed.

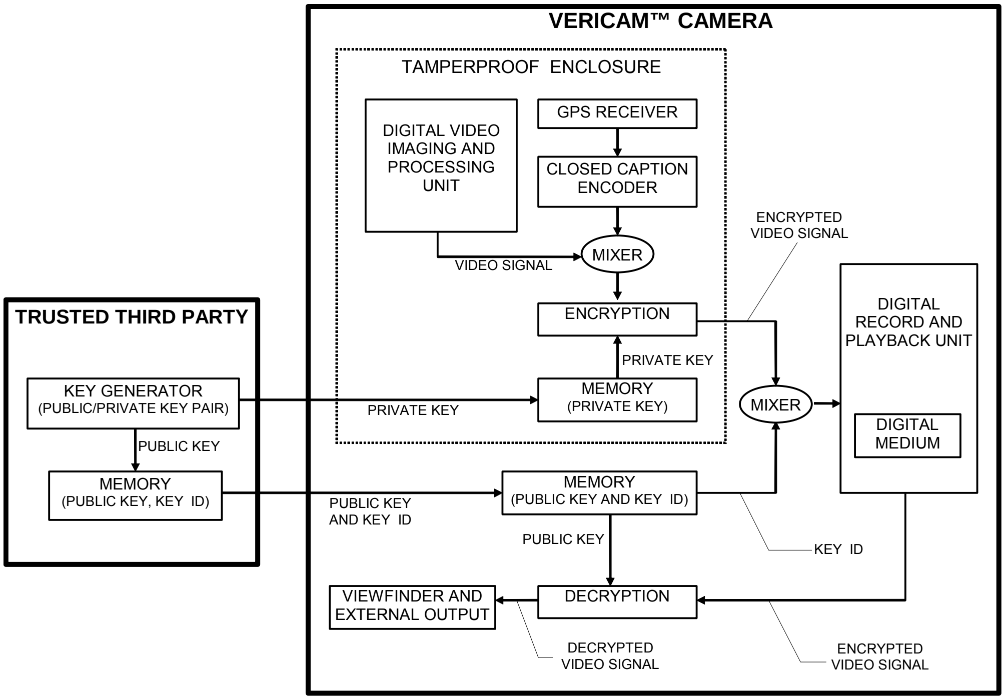

Figure 1. Block diagram overview of the public key Event Verification System.

The basic operation of EVS is simple. Using a private key supplied by a trusted third party, the Vericam™ video camera encrypts and records an event and also the time and place that it occurred. Time and location information are incorporated into the recorded data stream using a built-in Global Positioning System (GPS) receiver. Once recorded, the recording can only be decrypted, and thereby authenticated, with the public key supplied by the trusted third party. The only copy of the private key that is used for encryption resides in a tamperproof enclosure which, if breached, automatically destroys the key. Thus, without the ability to learn the private key, it is impossible for anyone to alter or forge information recorded by the Vericam camera. One advantage to employing public key encryption is that digital players can be manufactured to allow the playback of a Vericam recording by any independent party wishing to perform the verification process.

Using EVS, courts, government and intelligence agencies, news agencies, researchers, journalists, insurance agencies, private investigators, and others will be able to easily verify the authenticity of a recording, or make their own verifiable recordings. Furthermore, EVS technology can easily be applied to other fields including audio, biometrics, photography, file authentication, and finance.

Of course, the Event Verification System can't stop a resourceful party from staging an event. What it can do is to tell you when and where an event happened and that it occurred exactly as recorded. EVS is the next best thing to being there.

For more information on the Event Verification System contact
Harlan J. Brothers at (203) 589-6769 (harlan@brotherstechnology.com).

Applications of the Event Verification System

EVS and the Financial Services Industries

- Investment banks, commercial banks, stock brokerages, and consumer credit companies can benefit from their use of EVS to authenticate high-security transactions. Not only will transactions become absolutely tamperproof, but their sources could be unequivocally verified. An EVS system would be fully scaleable to handle everything from a single bulk sale transfer to distribution of single or fractional shares. EVS can also establish tamperproof audit trails. By securing the entire network, EVS can guarantee the underlying integrity, stability, and accuracy of any transaction.

- Consumer credit companies can insure the security of online purchases by using an EVS-based e-commerce cash box. This box would provide consumers and credit companies with the highest level of security and enable consumers to purchase items without placing their credit card numbers on the network.

EVS and Health Care

- Medical and insurance records can be authenticated and rendered tamperproof, thereby enhancing the integrity of the system and significantly bolstering indemnification against potential law suits.

EVS and Government

- Government records, including defense records and financial data, can be tamperproof. Their time and place of origin can be unequivocally established and audit trails can be verified.

- Authentication of satellite surveillance photos can be routinely carried out by the public-at-large thereby increasing the faith of the international community in reliability of U.S. government information.

- Electronic voting systems can be made inherently tamperproof and their results verifiable by any independent organization.

Other Applications of EVS

- Surveillance companies can create unalterable video and audio recordings. Such recordings would be inherently more valuable as evidence since their authenticity, along with the time and place they were recorded, will be established beyond doubt.

- Security companies using video or biometrics to prevent unauthorized access or entry can offer an increased and unprecedented level of authorization services to their clients. In addition, EVS would bolster indemnification and reduce written exposure to risk (settlement payments, lawsuits, etc.)

- Producers of intellectual property, such as inventors and software developers, can firmly establish their rights by authoring work on EVS-based computers.