SAND--90-0982C

DE90 013402

Modular Authentication Systems

Charles S. Johnson, W. R. Hale, and Dennis L. Mangan
International Safeguards Division, Sandia National Laboratories
P. O. Box 5800, Albuquerque, New Mexico 87185

Abstract

Authentication systems are required in situations where it is not necessary to protect the contents of the information but to verify the transfer of the information. The Modular Video Authentication System (MVAS) has been developed by Sandia National Laboratories to provide authentication of video signals in already-wired systems. The video authentication technique uses similar microprocessor circuitry at the transmission point, and at the receiving point, to select sample points from the video images for comparison. If a significantly different image was substituted, the comparison would fail at a number of points and the video image would not be authenticated. A similar system has been developed by Sandia for authenticating digital data transmissions. This system is used to determine whether any data alternation or substitution has occurred between the point of the data transmission and the point of the data reception. As with the MVAS, authentication equipment is required at both the transmission and receiving locations for the system operation. This paper describes both the video authentication system and the digital data authentication system, how authentication is accomplished, and how the systems interface with existing hardware.

I. Introduction To the Modular Video Authentication System

The Modular Video Authentication System (MVAS) has been developed to meet general system requirements for a method to authenticate existing video transmission lines. It requires installation of a Video Authentication Processing Module (VAPM) in the camera housing, and a Video Authentication Verifier Module (VAVM) at the receiving point of the video signal. These two modules are basically identical, except for different software and different programmable logic arrays (Figure 1). The modules are housed in aluminum anodized case with a sliding lid.

The Processor Module receives the video signal from the camera or other video source and inserts the authentication-related information into the video signal. Digital authentication data and digitally encoded video samples of the images are placed on lines 10 and 11 in the vertical interval of the video signal. The authentication process requires internal clock circuits in both modules, adjusted to the same time. Clock adjustments are accomplished through the use of an Authentication Programming Unit.

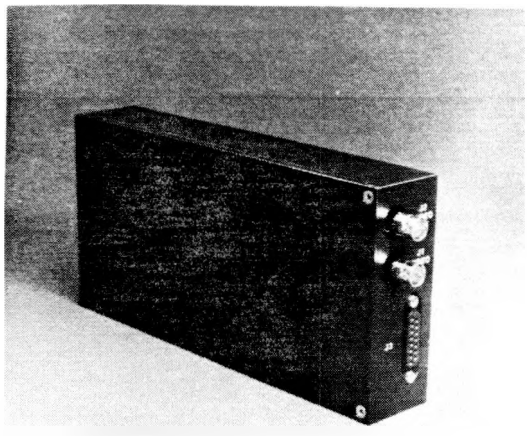

Figure 1

The VAVM receives a signal from the VAPM and processes it to determine if it is authentic. It receives digital information along with the video signal to determine which pixels to sample and compare. The VAVM sends out three signals that can be read by a computer-monitoring system, if desired. These three signals are: "Not authenticated," "System Problem Flag" and "Camera Housing Switch Open." The "Camera Housing Switch Open" signal is carried in the digital information sent from the VAPM and indicates that the switch monitoring the camera housing is open. The "Not Authenticated" signal means the system has not authenticated the video. The "System Problem Flag" means something is not working correctly in the system. The three signals are a condensed set of information that is inserted into the picture by the VAVM.

The VAVM has the additional feature to annotate on video the functional status of the system. It inserts a row of characters in the top of the output video image to show its operational status. These characters will be recorded any time the video is recorded. The characters that appear and their meanings are as follows:

---

* -- authentication in process
A -- Authenticated video
N -- Not authenticated video
S -- camera housing Switch open

The asterisk, "*", appears whenever an authentication session is in progress. The asterisk tracks the authentication indications of the LED of the transmitter VAPM. The purpose of the asterisk is to allow an observer to verify that the system is operating by noting that the asterisk turns off and on. The letter "A" appears to indicate that the last video sampled was authenticated. If the letter "N" appears, indicating that authentication did not occur, additional diagnostic indicators will appear. These indicators are:

F -- digital link Failure (no message received from the camera within 1 min)
D -- Digital authentication failure on the transmitted digital information
V -- Video authentication failure

The occurrence of the "D" signal will also invoke additional diagnostic indicators which can be analyzed as follows:

T -- Time comparison fail
L -- Link transmission count fail to check
C -- Calendar (date) comparison fail

The characters have fixed positions on the line that begin in the upper left hand corner of the screen. A string of characters would appear as:

AN*FVDTLC

Not all characters will appear together at the same time. If the characters should interfere with the display on the screen of other information of the system, they can be moved through software changes or inhibited so that they do not appear.

II. Circuit Operation

A block diagram of the authentication system is shown in Figure 2. This block diagram relates to both modules and can be used to explain basically the operation of the modules. The video from the camera enters the buffer amplifier of the module. The sync stripper removes horizontal and vertical information from the video signal. The video clamp circuit places the video from the buffer amplifier at a reference level. The sync signal is fed to the programmable logic arrays (PLA) and a phase lock loop provides a reference frequency at 80 times a horizontal frequency (HF). This 80 HF clock is fed to the PLA.

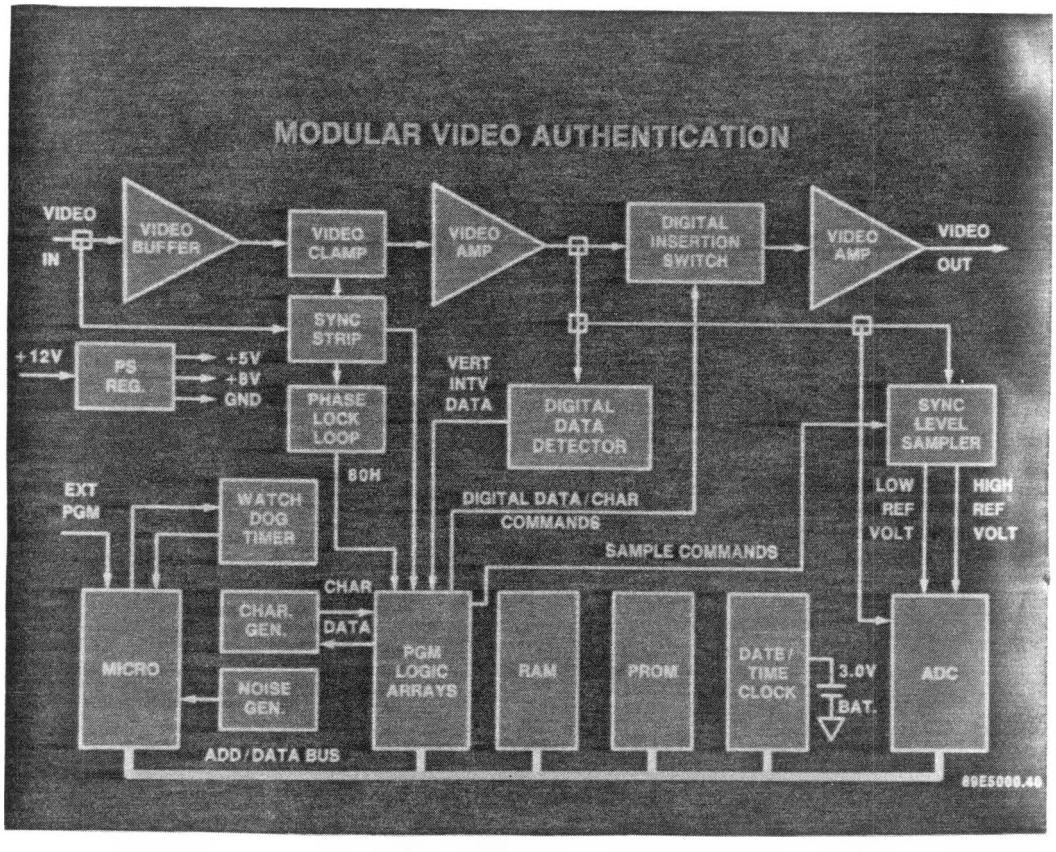

Figure 2

The output of the video clamp amplifier is fed to the video amplifier, which buffers the signal prior to insertion of the digital data or video characters. In the processing mode, the digital insertion switch inserts information on lines 10 and 11 of the video signal.

The Analog-to-Digital Converter (ADC) has its gain changed according to the amplitude of the sync level signal in the video. The sync level sampler circuit samples the sync tip and the black level and develops a low reference voltage and a high reference voltage which are fed to the ADC. If the video signal changes in a linear fashion, the sync part of the signal will vary accordingly. The ADC digitizes the video signal and its digital output remains the same, because the references voltages are changing in accordance with the sync voltage. The information for all the insertion comes from the microprocessor which is controlling the processing of the signal. The Random Access Memory (RAM) is used for program functions and for holding data prior to transmission. The Programmable Read-Only Memory (PROM) contains random number information. The date-time clock is an integrated circuit that has its own battery backup to enable the authentication modules to keep their time, even though 12 volt power is removed.

A hardware random noise generator creates random numbers for the microprocessor. The addresses for the PROMs are selected from a random noise generator and are not likely to contain any repeat information. The watchdog timer is used to insure that the microprocessor does not jump into some forbidden area of memory and not return.

Video is authenticated in 256 frame authentication sessions that occur every 30 seconds. A video sample is taken in Field 1 of each video frame and transmitted on line 11 of Field 2. The modules at the transmission and receiving ends of a link sample at the same time. After the completion of the 256 samples has occurred, a comparison is made by the VAVM to determine if the authentication process has taken place correctly.

The system has a number of features to protect against tampering. Failure of the digital data link will prevent video authentication from taking place. The date-time clock prevents insertion of old data into the operation of the video authentication modules. The time data change constantly and are authenticated within the digital authentication algorithm after each transmission.

III. Digital Data Transmission Authentication Techniques

The digital information is multiplexed onto a transmission line of any type, be it hardware, fiber optics, or RF. The digital data transmission format is organized as shown in Figure 3. The format of the data is important but the essential element of the authentication technique is a Programmable Read-Only Memory (PROM).

A group of words at the beginning of the data format are synchronization words and provide a handshake between the transmitting and receiving devices. The first five bytes define the beginning of the transmission. These bytes are followed by PROM addresses which show the addresses of four different randomly chosen locations in the memory. By taking the 32 bits referenced by these addresses, a Random Authentication Number (RAN) is developed. It forms the basis of the authentication algorithm. The next group of data is date and time, followed by data words, etc., as indicated in the figure.

Authentication is accomplished by taking the incoming information as displayed in the data format and performing the authentication algorithm in the receiving module. Once the authentication algorithm, which is based on the RAN, has been performed, a comparison of the genuine authentication bytes received with the ones determined by the receiver will verify that the data is correct. Substitution of different data, memory, addresses, time and date will be, with a very high probability, detected by the authentication algorithm.

This authentication technique is capable of being implemented by today's technology without the use of sophisticated data encryption algorithms or hardware. The number of different PROMs that can be produced are virtually endless. The PROMs can be produced and controlled with relative ease.

Administrative control of the RAN PROM starts with the generation of the random numbers in a computer. Once a file of random numbers has been generated the file can be transferred to the PROM, or it can be transferred to a disk. The approach utilizing the random number PROM is expandable to a number of different ways for future use.

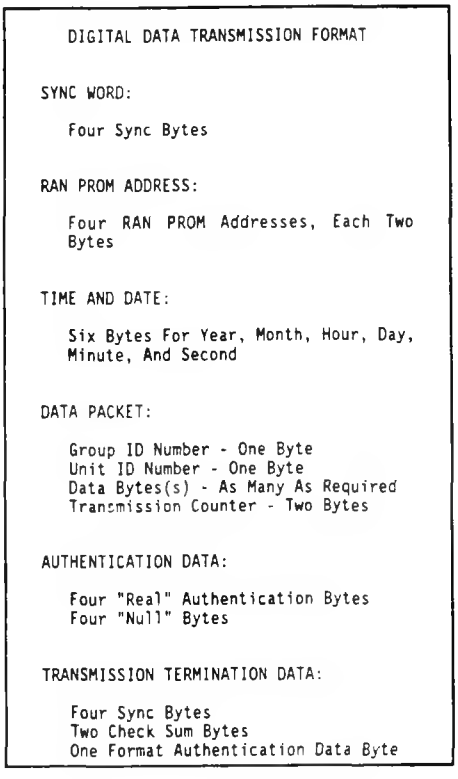

Figure 3

Summary

In this paper we have discussed a video authentication system which was designed to provide a capability to authenticate video transmission links. The system provides on the screen status and digital output. The modular approach allows it to be added to most video transmission systems in use today.

The digital data authentication format is being used in a number of authentication systems and is planned for further use in safeguards and security equipment. The importance of authentication of data and images will grow as the technology base makes it easier for adversaries to change information that is an important part of security systems.