

Information Security for Mitsubishi Digital CCTV System MELOOK μ

Authors: Teruyoshi Yamaguchi*, Hironobu Abe* and Tomohiro Ueda**

1. Introduction

Mitsubishi Electric has developed a new digital closed-circuit television (CCTV) system MELOOK μ featuring the simple introduction of a video surveillance system, and an easy-to-use video information management system. MELOOK μ not only records and displays high-definition images, but also protects against eavesdropping of stored images through the use of Mitsubishi Electric's encryption technology MISTY. This paper presents the security features of MELOOK μ .

1. Mitsubishi Digital CCTV System MELOOK μ

1.1 Configuration of MELOOK μ

The digital CCTV system MELOOK μ consists of a mega-pixel recorder, up to eight mega-pixel cameras, and up to eight units of DIGITAL MELOOK series network cameras. The mega-pixel recorder is connected with these cameras to collect, store and display video images. The mega-pixel cameras are directly connected to the mega-pixel recorder, whereas the DIGITAL MELOOK series network cameras are connected to the recorder via a switching hub. Video images stored in the recorder can be copied to DVDs as required. (Fig. 1)

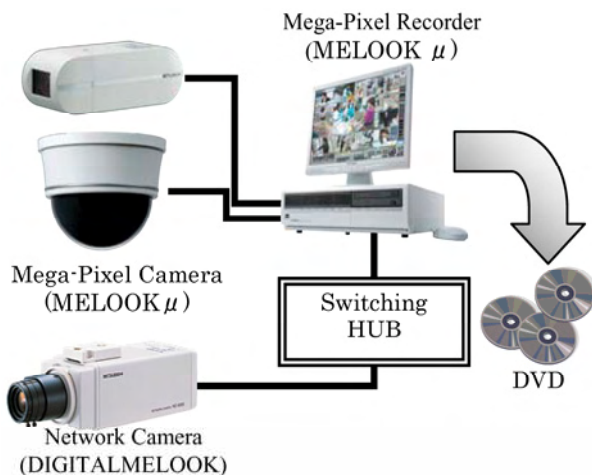


Fig. 1 Mitsubishi digital CCTV system MELOOK μ

1.2 Security features of MELOOK μ

MELOOK μ encrypts captured video images in real time before storing them to protect the accumulated data. When encrypted video images are displayed, they are decrypted in real time. They are copied to DVD or

other media as encrypted. Since the video images are encrypted when stored, they cannot be directly viewed with an ordinary file viewer unless a legitimate method is used. As a result, even if a DVD or HDD is stolen, the stored video information is protected. (Fig. 2)

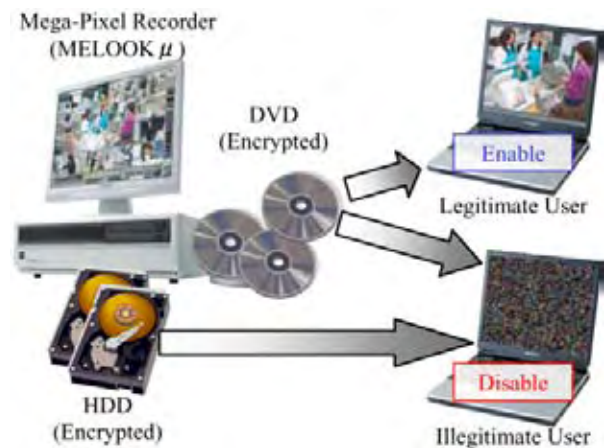


Fig. 2 Image data encryption in MELOOK μ

In addition, the mega-pixel recorder performs user authentication to control access. The access control function restricts user's operations. Access to the DVD data is available by proprietary viewer software, which is included when the video images are copied to DVD. User authentication is also performed when a DVD is played back. (Fig. 3)

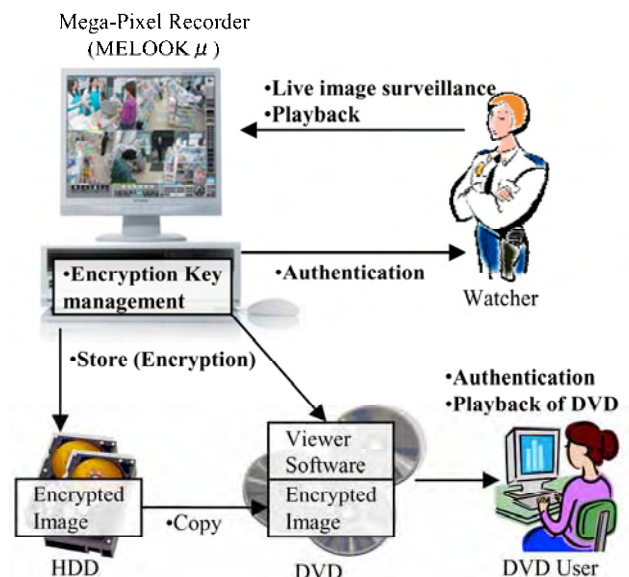


Fig. 3 Security functions in MELOOK μ

2. Security Technologies in MELOOK μ

2.1 Encrypted storage

In a digital CCTV system, a large amount of video data captured by camera must be stored and displayed at a high speed. MELOOK μ encrypts mega-pixel quality (SXVGA, Super Extended Video Graphics Array) video data for storage, and decrypts it for display. As a consequence, high-speed encryption and decryption are required.

The MELOOK μ requires a cryptographic performance of 80Mbps¹ at maximum. In addition, MELOOK μ must perform other processing tasks besides cryptographic processing. Therefore, the load of cryptographic processing should be kept as low as possible. Generally, it is necessary to use dedicated hardware to meet these requirements.

To realize low-cost cryptographic equipment by achieving hardware-level performance using a software process, Mitsubishi Electric has developed a new cryptographic algorithm, BROUILLARD, which belongs to the MISTY family and provides both high-speed processing and sufficient security.

BROUILLARD achieves high-speed and secure operation by means of random access within a large memory space. BROUILLARD realizes an encryption speed of 8 Gbps through implementation on the Pentium 4 (3 GHz).

MELOOK μ applies BROUILLARD to realize an encryption speed of 80 Mbps through software.

2.2 Encryption key management

The mega-pixel recorder encrypts and accumulates video image data in mass storage, and strictly controls the key information used for encryption as well as provides authorized users with easy-to-use key information.

The mega-pixel recorder randomly generates image encryption key when the system is initially booted up, and thus the probability that two recorders have identical key is extremely low. With this mechanism, video images encrypted on a certain recorder cannot be opened on other recorders. The image encryption key generated in this manner is encrypted by multiple parameters and stored in multiple non-volatile areas. The encryption keys stored in the non-volatile areas are all encrypted and thus secure against illegal extraction of data from non-volatile areas.

When the mega-pixel recorder is booted up in a normal mode, encrypted image encryption key is retrieved from the system area and decrypted. Using the decrypted image encryption key, the video images are actually encrypted.

When a user copies their images to DVD, the en-

rypted image encryption key, encrypted images, and viewer software are copied. When the DVD is replayed, the viewer software is activated, and then the password is entered. If the entered password is correct, the image encryption key is decrypted, then the encrypted images are decrypted and played back. If the password is invalid, the image encryption key cannot be decrypted, inhibiting the playback of encrypted images. (Fig. 4)

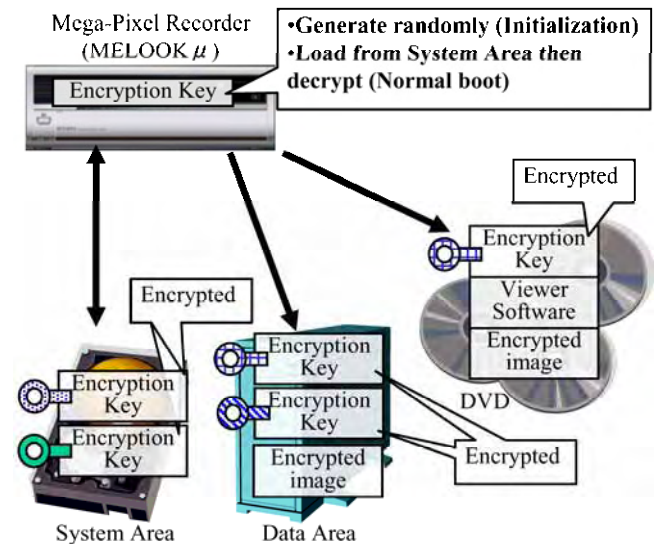


Fig. 4 Encryption key management in MELOOK μ

2.3 User authentication

The mega-pixel recorder performs access control by verifying the password provided by the user.

Table 1 shows the user levels and operations permitted for each level. Assistant level allows only live image surveillance. Manager level allows, in addition to live image surveillance, playback of accumulated images, and camera manipulation. Owner level is the highest authorization level and allows changes to various settings and copying of DVDs. Operations at the assistant level do not require a password, whereas operations at the manager and owner levels require password verification.

Table 1 User's authority and available operations

Authority	Available operations	Password
Lv.1 (Assistant)	•Live image surveillance	Unnecessary
Lv.2 (Manager)	•Live image surveillance •Playback •Camera manipulation	Necessary
Lv.3 (Owner)	•Live image surveillance •Playback •Camera manipulation •Configuration •Copy to DVD	Necessary

¹ Including both encryption and decryption

A password for DVD playback is defined when the owner copies video images to DVD. When the DVD is played back, the specified password must be entered to play back the video images.

A manager level or owner level password can be changed after it is authenticated at each proper level.

3. Conclusions

This paper introduced the security features of the Mitsubishi digital CCTV system, MELOOK μ . In the future, MELOOK μ is expected to be equipped with additional features including Web distribution functions, and backup HDD expansion capability.