

Intelligent Footage Information Security Solution to Protect Footage and Personal Privacy



INDEX



01. Introduction

02. Overview

03. Main Functions

04. System Specification and System Overview



Intelligent footage information security solution to
protect footage and personal privacy



01. Introduction

Introduction

Personal Information Protection Act

- ✔ Personal information means the information relating to a living individual and includes the information that identifies a particular individual (example: name, resident registration number)
- ✔ The law establishes a legal framework of regulations to protect personal privacy and enhance the protection of individual rights and interests *(Enacted on March 29, 2011).
- ✔ Purpose: This Act was stipulated to regulate the processing of personal information in order to promote the rights and interests of individuals by preventing the collection, leakage and abuse of personal information, and furthermore to protect an individual's dignity and values
- ✔ Article 25 (Restrictions on Installation and Operation of Footage Information Processing Device): Operators of footage information processing devices shall take measures to ensure security according to Article 29 to prevent personal information from being lost, stolen, leaked, forged or damaged (Revised on 07/24/2015)

Measures are required to prevent personal information leakage, forgery, tampering, etc.

Guidelines on the installation and operation of footage information processing devices for public institutions


- ✔ (Use of footage information in compliance with purpose of use and provision to third parties) Public institutions can use personal footage information in compliance with the purpose of use if a footage information processing device is installed and operated in an open public place due to the reasons under Article 25 of the Act, and it can also provide the information only in certain circumstances.
- ✔ (Use of footage information other than for the purpose of use and provision to third parties) Public institutions may not use personal footage information or provide it to third parties other than for the purpose of collection, unless it is stipulated by law
- ✔ (Storage and destruction) The footage information collected by a footage information processing device shall be immediately removed after the retention period specified in the management policy for a footage information processing device. However, exceptions apply if there are special regulations in other laws.
- ✔ (Measures to secure the security of personal footage information) The heads of public institutions shall seek measures to secure the security of personal footage information so that it is not lost, stolen, leaked, forged, or destroyed.

Management plans are required to ensure the safe use of footage information in compliance with the purpose of its use



SECUWATCHER for CCTV conducts a safe footage export management based on real-time privacy protection and prevention of footage forgery and its encryption, ensuring compliance with Personal Information Protection Act and safe management of footage information





Intelligent footage information security solution to
protect footage and personal privacy

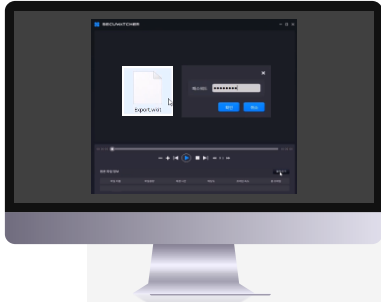
 **SECUWATCHER**

02. Overview

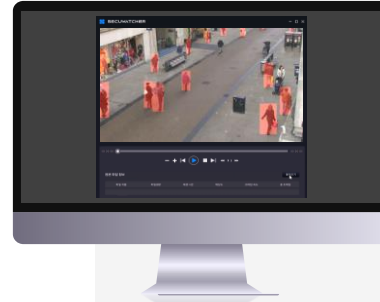


Overview

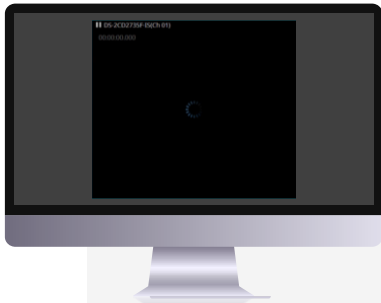
"A CCTV footage information security solution that supports **footage encryption** and **export** in order to **protect footage** and **personal privacy**"



Safe
footage export
management




De-identification
using **object**
detection, tracking
and **masking** functions



Lightweight
encryption algorithm-
based **high-speed**
encryption/decryption
of footage



Prevention of
footage forgery and
tampering using
watermarks



Intelligent footage information security solution to
protect footage and personal privacy



03. Major Functions

Major Functions

01 – Footage export function

Detailed Functions

- 1 Footage export settings:** Provide functions of masking range and method setting (mosaic or blur), **watermarks** setting and Dat setting
- 2 Footage export:** File storage method setting (source file or encryption), DRM setting (number of plays and duration)
- 3 Completion of footage export :** Footage export to the outside
- 4 Selection of the exported footage and input of decryption key:** Allow to enter the key value for the selection of the footage and the decryption of the encrypted footage
- 5 Viewing exported footage:** Exclusive player-based viewing of the footage

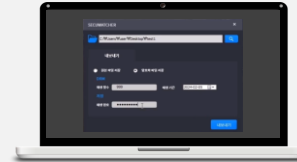


Expected Effects

- ▶ **Enable prevention of footage forgery and tampering, as well as safe export of footage**, using footage encryption, masking, DRM and watermarks
- ▶ **Footage access control for unauthorized persons** with exclusive player-based viewing of export footage



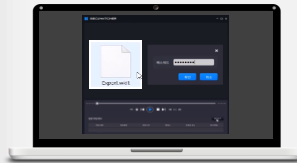
① Setting footage export



② Exporting a footage



③ Completing footage export



④ Selecting the exported footage and filling in the decryption key



⑤ Viewing the exported footage (exclusive player)

Major Functions

02 – De-identification function (detection and masking)

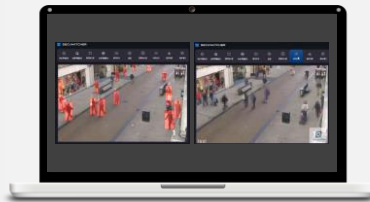
Detailed Functions

- ✓ **Automatic object tracking, detection and masking:** Allow automatic detection of moving objects in footage (people, cars)
- ✓ **Manual object tracking, detection and masking:** Masking continues as long as the mouse click time
- ✓ **Selected area masking:** Select a certain area and mask the corresponding area
- ✓ **Selected object tracking, detection and masking:** Detect, track and mask the selected object automatically

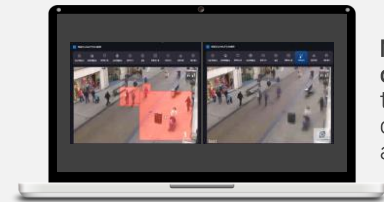


Expected Effects

- ▶ Ensure **perfect protection of personal privacy** using object detection/masking-based **de-identification**
- ▶ **Expected to increase user satisfaction by providing various types of detection and masking functions**



Automatic object tracking, detection and masking



Manual object tracking, detection and masking



Selected area masking



Selected object tracking, detection and masking

Major Functions

03 – Footage encryption/decryption and the prevention of forgery and tampering

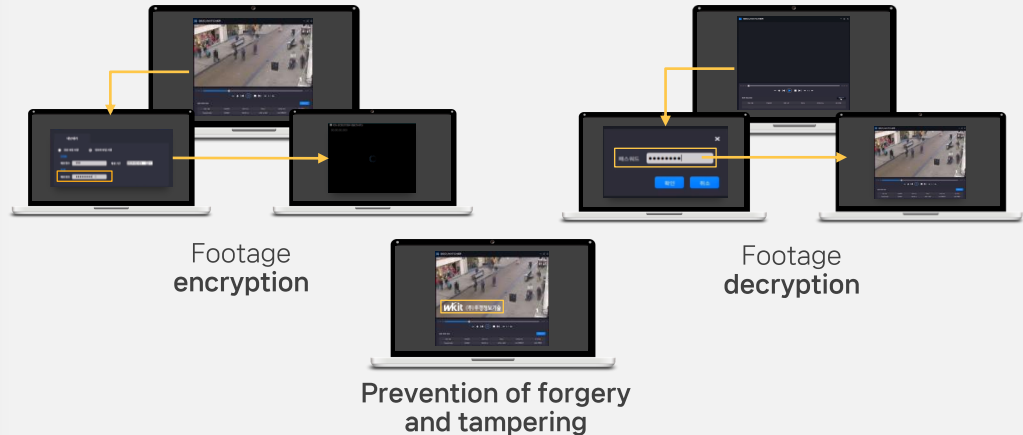
Detailed Functions

- ✓ Allow **encryption** after setting a **password** in order to restrict access to footage by unauthorized users in exporting the footage
- ✓ Lightweight encryption algorithm-based **real-time high-speed encryption**
- ✓ Allow **exclusive player-based** viewing of source footage **only after entering the password set in decrypting** the encrypted footage
- ✓ Insert **watermarks in the form of images and text** into footage to prevent forgery and tampering



Expected Effects

- ▶ **Enhance security** with encryption/decryption of footage files
- ▶ Digital watermarking technology **enables to claim ownership of footage** in the event of footage forgery, tampering and abuse





Major Functions

04 – Footage editing function

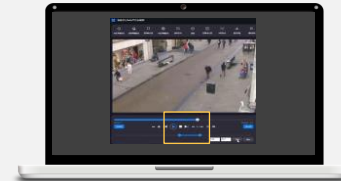
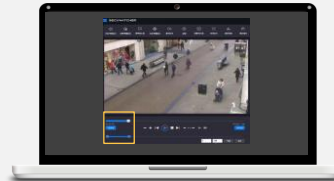
Detailed Functions

- ✓ The footage cropping function **allows users to extract only the specific area they need**
- ✓ Footage pasting function allows **a user to connect images they need**



Expected Effects

- ▶ **Enable to apply de-identification, forgery and tampering prevention, and encryption for only the area a user needs** using the footage editing function



Footage
cropping



Footage
pasting

Major Functions

05 – Statistics function

Detailed Functions

- ✓ Allow to view **the history of footage export, all members and CCTV information, etc.** on the statistics main screen
- ✓ **Provide statistics** by month, day, region, and application reason



Expected Effects

- ▶ Help to **derive insights** through the analysis of usage based on statistical data



Monthly statistics



Daily statistics




Regional statistics



Application reason statistics



Statistics main screen



Intelligent footage information security solution to
protect footage and personal privacy



04. System Specifications & System Overview

System Specifications and System Overview

System Specification

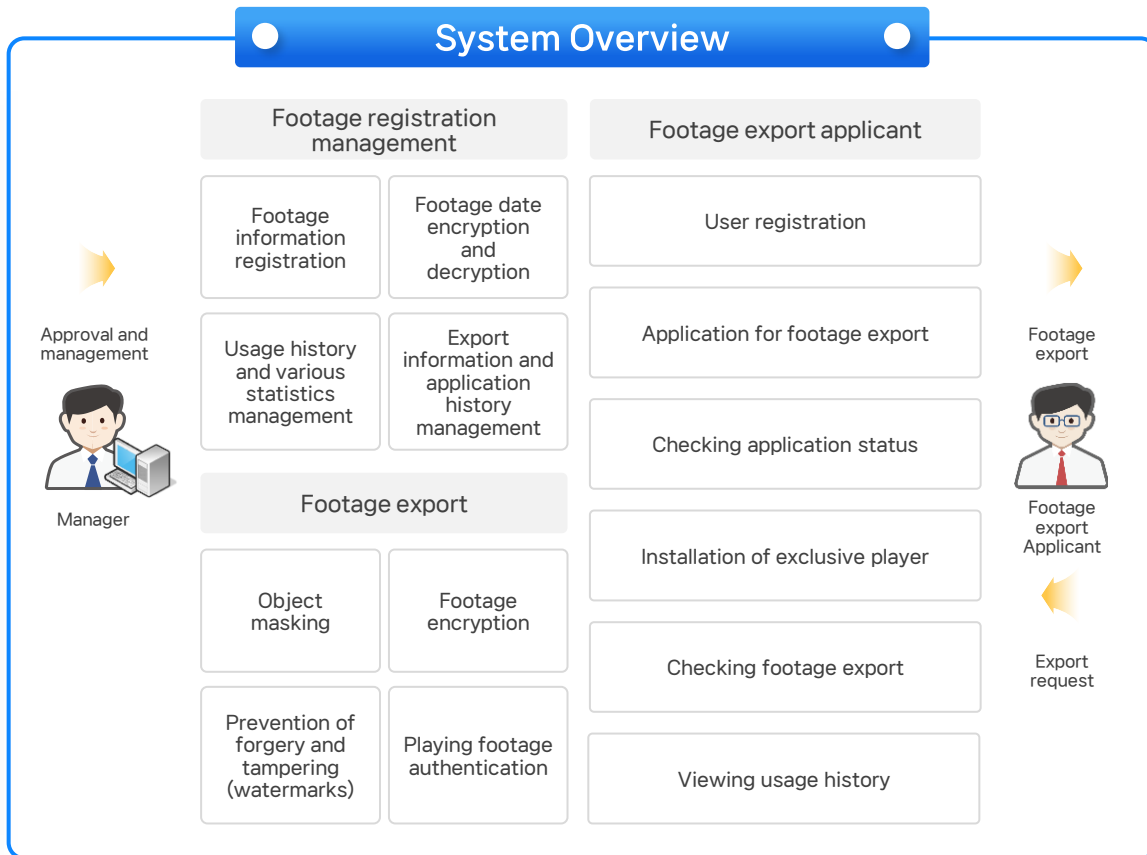
✓ Operation environment

- ▶ Server environment
 - Windows Server 2012 or later version
- ▶ Client
 - Windows 7~10 (32, 64bit)
 - Explorer, Chrome support

✓ Minimum/recommended operating specifications

- ▶ S/W - Web
 - CPU: Intel® Xeon 2234G (4Core, 8Thread, 3.6 GHz)
 - RAM: 8 GB or higher
 - HDD: 4 TB or higher
 - OS: Win server 2019 Standard (16Core, 5CAL)
 - DB: MariaDB
- ▶ S/W - Export
 - CPU: Intel Core i7 or higher
 - RAM: 16 GB or higher
 - SSD: 512 GB or higher
 - GPU: GTX 2000 series, VRAM 8 GB or higher
 - OS: Windows 10 pro 64bit

System Overview



We live on SPHERE : AI Xperience



wkitglobal@sphereax.com | www.sphere.com