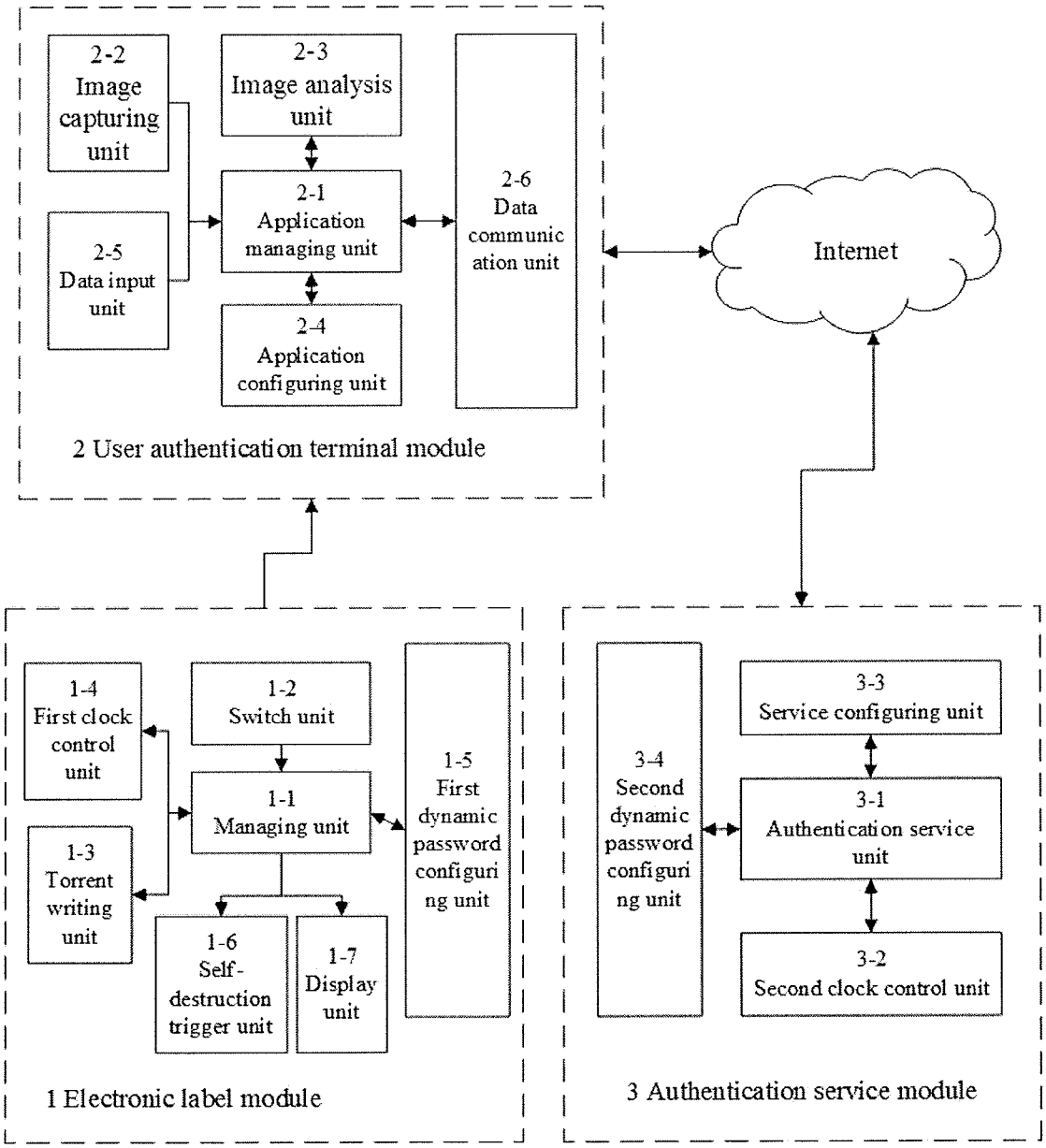
2-2
Image capturing unit
2-3
Image analysis unit
2-1
Application managing unit
2-6
Data communication unit
2-5
Data input unit
2-4
Application configuring unit
2 User authentication terminal module
Internet
1-4
First clock control unit
1-2
Switch unit
1-5
First dynamic password configuring unit
1-1
Managing unit
1-3
Torrent writing unit
1-6
Self-destruction trigger unit
1-7
Display unit
1 Electronic label module
3-4
Second dynamic password configuring unit
3-3
Service configuring unit
3-1
Authentication service unit
3-2
Second clock control unit
3 Authentication service module

Fig. 1

S201: assigning a unique ID number to each electronic label module, wherein the ID number is expressed as IDS1, and is located on the surface of the electronic label module. An identical clock accumulating cycle is defined in the electronic label module and the authentication server module. The product information and related information are written into a service configuring unit. A torrent file for associating the electronic label module with the authentication service module is defined. Saving the data TDSH in the application configuring unit represents that a self-destruction device of the electronic label module has been damaged. The PSW field is written into the record corresponding to ID number IDS1 in the service configuring unit.

S202: turning the electronic label module on via the switch unit. Then the torrent file is written via the torrent writing unit, meanwhile, the torrent file is written into the record corresponding to the IDS1 in the service configuring unit of the authentication service module through the internet.

S203:turning the electronic label module on via the switch unit. The mange unit detects whether the self-destruction trigger unit is damaged. If the self-destruction trigger unit is damaged, the electronic label module outputs the specific data TDSH via a display unit, representing that the electronic label module has already stopped working. If the self-destruction trigger unit works properly, the managing unit of the electronic label module initializes the clock data to DSS1 at the first clock change cycle according to the clock change cycle of a clock control unit. The managing unit uses the clock data DSS1, the random number RandomD, the ID number IDS1 of the electronic label in the torrent file, as calculation factors, to generate a dynamic password data DKS1 by a dynamic password generating algorithm PSW1 of a first dynamic password configuring unit. Then the first dynamic password data DKS1 is displayed on the display unit. Then the managing unit accumulates the initial clock data DSS1 to obtain the DSS2 according to the predefined clock accumulating cycle. Then the DDS2 is saved in the cache.

S204: capturing, via the image capturing unit controlled by the application managing unit of the user authentication terminal module, the image data TDT1 of the electronic label module, wherein the image data IDT1 of the electronic label module comprises the dynamic password data displayed on the display unit, and the ID number IDS1 of the electronic label module located on the surface of the electronic label module. The application managing unit of the user authentication terminal module locates, segments, and analyzes the image data IDT1 via the image analysis unit to obtain a dynamic password data DZXS displayed on the display unit of the electronic label module and the ID number IDS1 of the electronic label module. Then searching is conducted in the application configuring unit. If the DZXS equals to the TDSH, which indicates that the self-destruction device of the electronic label module is damaged, the authenticating process ends. If the DZXS does not equal to the TDSH, the IDS1 is saved into the application configuring unit. The IDS1 and the DZXS are sent to the authentication service module via the data communication unit connected to the internet.

S205: receiving the data IDS1 and the DZXS sent from the user authentication terminal module. Subsequently, the authentication service unit searches the record corresponding to the IDS1 in the service configuring unit using the IDS1, and extracts the dynamic password generating algorithm PSW2 adopted by the electronic label module represented by the clock data DSS1, the random number RandomD, and theIDS1 that are initially written into the torrent file. Then the authentication service unit obtains the system time RSS1 of the current authentication service module, and subtracts the DSS1 from the RSS1 to obtain a result. The result is divided by the initially defined clock accumulating cycle to obtain the RZSC which is the number of times the electronic label module accumulated in accordance with the clock accumulating cycle. Finally, the dynamic password data RKS1 is calculated using the RandomD, the DSS1, the RZSC, and the IDS1 as calculation factors through the dynamic password generating algorithm PSW2 of the second dynamic password configure unit.

S206: the authentication service unit compares the calculated RKS1 with the DZXS. If the RKS1 equals to the DZXS, the result indicating that this electronic label module is valid is sent to the user authentication terminal module through the internet If the RKS1 does not equal to the DZXS, the result indicating that this electronic label module is not valid is sent to the user authentication terminal module through the internet.

S207: after the user authentication terminal module receives the result fed back from the authentication service module, the user authentication terminal module displays the result, so as to complete this validity authentication process with respect to the electronic label module.

Fig. 2

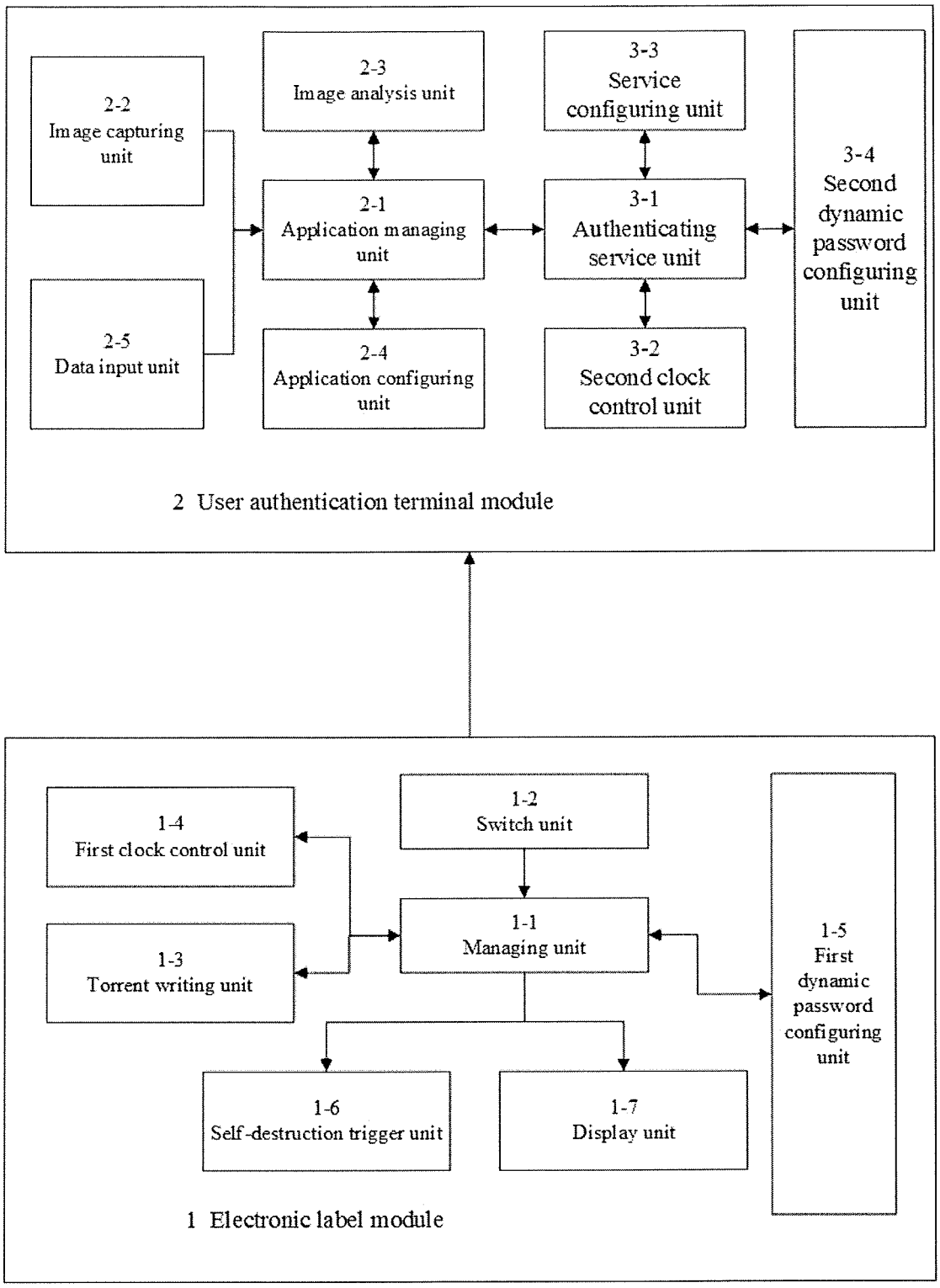
2-2
Image capturing unit
2-3
Image analysis unit
3-3
Service configuring unit
3-4
Second dynamic password configuring unit
2-1
Application managing unit
3-1
Authenticating service unit
2-5
Data input unit
2-4
Application configuring unit
3-2
Second clock control unit
2 User authentication terminal module
1-4
First clock control unit
1-2
Switch unit
1-1
Managing unit
1-5
First dynamic password configuring unit
1-3
Torrent writing unit
1-6
Self-destruction trigger unit
1-7
Display unit
1 Electronic label module

Fig. 3

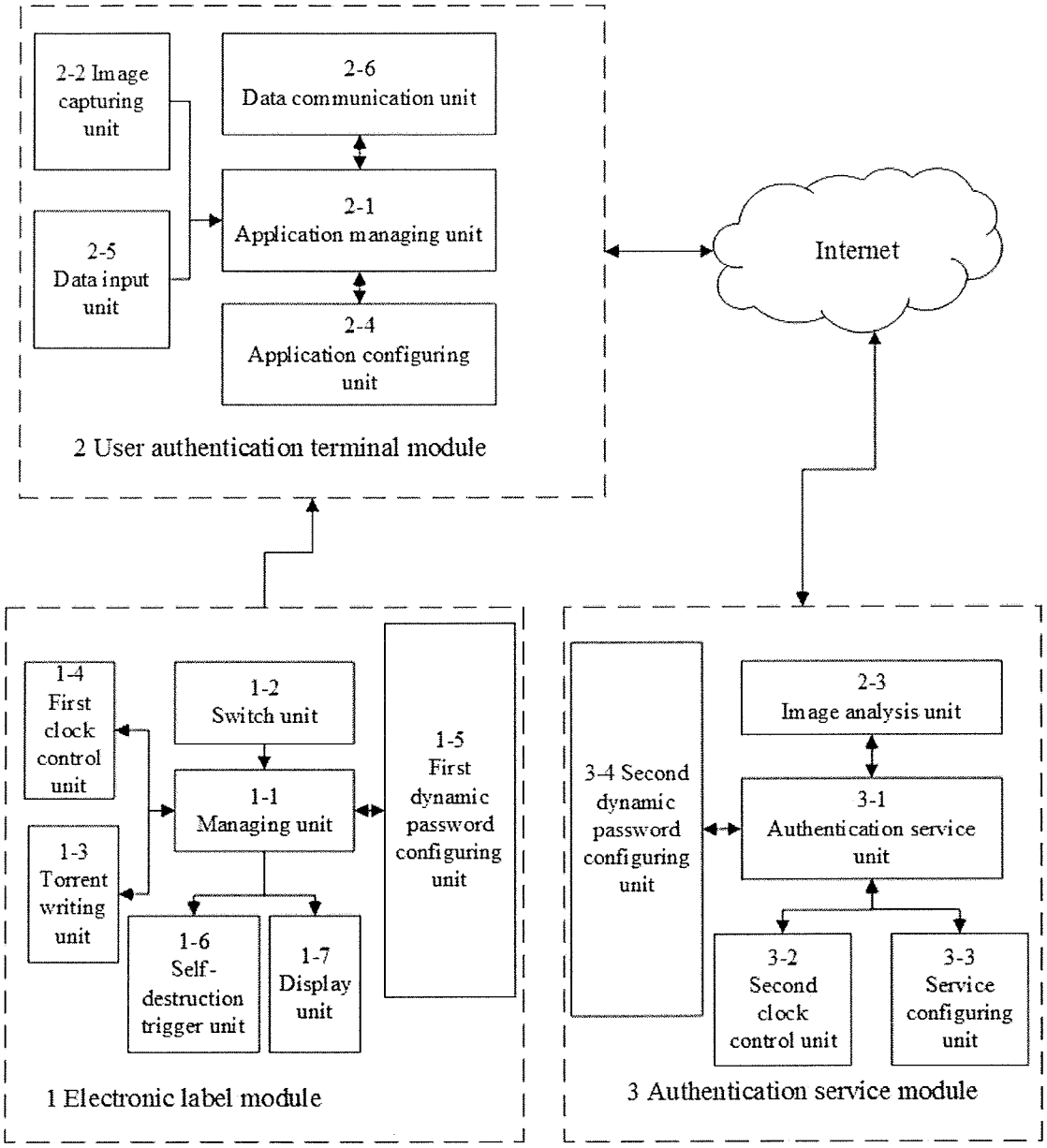
2-2 Image capturing unit
2-6 Data communication unit
2-5 Data input unit
2-1 Application managing unit
2-4 Application configuring unit
2 User authentication terminal module
Internet
1-4 First clock control unit
1-2 Switch unit
1-5 First dynamic password configuring unit
1-1 Managing unit
1-3 Torrent writing unit
1-6 Self-destruction trigger unit
1-7 Display unit
1 Electronic label module
3-4 Second dynamic password configuring unit
2-3 Image analysis unit
3-1 Authentication service unit
3-2 Second clock control unit
3-3 Service configuring unit
3 Authentication service module

Fig. 4