Encryption on the Capture DVRs – Chained Fingerprint

"Chained-Fingerprint" is an algorithm developed by Capture to protect the recorded images from illegal editing. This technology is based on the so called "Fingerprint Method" that extracts the unique summary of the given image. In that sense, the "Fingerprint method" is similar to a well-known technique know as "Message Digest (MD5)" that is generally applied to digital messages such as Email. As a matter of fact, IDIS uses MD5 at the base of Chained-Fingerprint.

A brief description of the "Fingerprint Method" is as follows:

1. Capture and compress the image.
2. Produce a 128bit code from the compressed image and other related data using MD5. We call the code "Fingerprint" of the image.
3. Save the "Fingerprint" with the compressed image and the related data. Once the "Fingerprint" is saved with the original data, it can be used to check if the original data has been modified or not a follows:

    a. Load the data to be tested.
    b. Produce "Fingerprint" of the data.
    c. Compare the "Fingerprint" to the saved one.

4. If both of them match, we can guarantee that the data is not modified because it has been proven that making the same 128bit code from different sources or generating source from the code is almost impossible.

The algorithm can investigate not only the image but also the information related to the image such as time captured, etc.

Watermark

While the "Fingerprint method" extracts and saves the unique summary of the original image, "Watermark method" mixes a specific image called "Watermark" with the original image.

Applying the reverse process of mixing can retrieve the watermark and the original image. The algorithm concludes that it is not modified when the watermark is extracted and it has not been modified.

Chained-Fingerprint

Even though the "Fingerprint method" is very safe and reliable, it has a small flaw. If someone (possibly the developer of the program) wants to edit the saved images, he can create a new image with the same fingerprint using the same program (since he developed that program) and overwrite the results of the original Fingerprint. The "Watermark method" has the same flaw.

Our "Chained-Fingerprint" has been develope to overcome this situation. In pure

Fingerprint, each fingerprint is independent of the other, since only a compressed image and some information related to the image are fed as inputs. However, in the "Chained Fingerprint", the fingerprint of the previous image is also fed as an input. As a result, all the images in the database are linked and one would have to edit all the images if they want to edit only one.

MD5

MD5 technology was developed at MIT (Massachusetts institute of Technology). It produces a 128bit code called "Message Digest" of "Fingerprint" from the input of arbitrary length. It has been proven that producing another input stream having the same "Message Digest" is impossible.

< home   < back to tech tips