Framework of Trustworthy Digital Photo Management System

Norishige Morimoto, Kohichi Kamijoh, and Akio Koide
Tokyo Research Laboratory, IBM
Kanagawa, Japan

Abstract

This paper describes technologies and framework for assuring the origin and integrity of photographs used in enterprise's business applications. The proposed framework is a combined process of cryptographic key management and a watermark technology, creating a secure end-to-end photo transaction. The solution involves digital camera manufacturers who supply asymmetric (public) keys for the cameras, the originators of the photographs, who take the pictures, and the enterprise application systems for the photographs, which generate and transmit encrypted symmetric keys to control the verification process assuring the integrity of the photographs. We use an automobile insurance claim process as a pilot application model to discuss the proposed framework, and implementation.

Introduction

Digital photograph became more and more popular as the price of the digital camera goes down. The total volume of the sales of the digital camera reaches to 10million units world wide in 1999. The use of digital photo including consumer application and business application. Use of digital photo improves efficiency and reduces costs in many business applications comparing to the traditional chemical photographs. No more D.P.E. cost, no more thick and awkward albums, and no more mailing process to transmit the photos. And mostly, no waiting time. They can be easily transmitted anywhere and can be easily retrieved from stored files. You can print whenever you want. However, for some serious business applications, this handy piece of information could be dangerous. Digital photographs can be easily manipulated and altered without leaving a trace. And if the application rely on the image as evidence, we had better to have some technical solution and framework to protect the photos from such kind of potential risks.

In order to create a trustworthy content, we should be able to identify the origin and the integrity of the content by using some kind of cryptographically trustworthy method.

a. Origin Identification

This is to allow the recipient of the content to identify the origin of the content. i.e. identify the device that was used to take the subject photos, or the photographer of the pictures.

b. Integrity Verification

This is to allow the recipient of the content to be able to verify the integrity, and detect unauthorized manipulation to the image, i.e. whether of not the image has been altered.

In this paper, we describe a proposal of technical solution and framework for a trusted digital photograph transaction process for the use of business applications. The solution addresses the following user requirements;

1. The solution covers the end-to-end photograph transmission path from digital camera to image database of enterprise photo application system.
2. The solution is simple and flexible, so that it can be widely accepted and used by all participating parties. It also does not add burden to the intermediate device or application, which is not a part of beneficiaries of the additional features.
3. The security features are implemented as a hidden feature to the content that is in existing standard format, so that the new feature is enabled in the new system, while the content will still be compatible to the legacy applications.
4. The solution must have reliable security features, and the primary beneficiaries (ex. users of the photo) should have control to determine the method and level of security.

Public Key Algorithm and Watermark Technology

The key technical elements for realizing the above requirements are public key encryption algorithms and digital watermark technology.

Public key encryption algorithms, also known as asymmetric key algorithms, are useful to allow multiple users to participate in the secure verification of the photos, and identify the originated device such as a digital camera or a scanner. The content will be signed digitally by using a device key, which is assigned uniquely to each individual device at the time the content is created (or captured). A complimentary pair of the public key will then, be distributed to the recipients of the content, which to be used to verify the authenticity (originality) of the content. The advantage of the asymmetric key algorithm is that, the one could not create a fake signature using the knowledge of the public key, so that the verification system remain secure, even disclosing the complimentary public key to the public. Further, the devices can establish exclusive and secure communication channels with multiple application systems by accepting an independent session key from each system, which is encrypted using a public key. Using session keys the single camera can create a different digital signature for different photos that can only be verified by a specific designated system.

Digital watermark, also known as DataHiding, is a technique to enable multimedia contents to carry an additional information without changing the size, format or visual quality of the content. In general, this invisible (and inaudible) data can also survive image compression, editing, encryption/decryption, and even digital/analog conversion in some cases. Therefore, it is an ideal way to carry the digital signature in an open system environment, where the image format may be changed by an innocent third party in between the sender and the receiver of the content. On the other hand, for some specific applications, the watermark will be made to be very sensitive to a very small modification. This can be used to detect the alteration occur to the image, or to identify the location that has been changed from the original watermarked content. Digital signature embedded into the image using this type of watermarking technology is a very powerful tool for the user of the content to, not only verify the integrity of the image, but also identify the section in the image that the modification is applied. The data embedded by watermark can only be read by the watermark data retrieval tool, with a proper watermark key. By exchanging the watermark key with a designated party, we can establish an exclusive content authentication channel, which is invisible to the outside world that is irrelevant to it. Since the data is hidden in an invisible and passive manner, it will not disturb the legacy application, nor obsolete platforms of applications that are used today. Therefore, maintain the compatibility, yet bring in a new and advanced security features to the digital content.

SIMON

In 1998 we had developed a prototype called Secured Image Management system ON Notes (SIMON)[1,2] and conducted a joint evaluation project using this system with one of the largest automobile insurance companies in Japan. The insurance company used to use analog photos for the remote damage estimation for the claims made by repair shops. By replacing to the digital photo, the company could save significant amount of time, cost for the processing of the photos, and improve the turn-around-time of the claim processing time, to gain higher customer satisfaction. On the other hand, the company does not want to be fooled by any forged image, which could give them very bad reputation in the marketplace. Therefore, it is essential to be able to identify unauthorized alteration or modification to the digital photo that they use for the claim estimation. The process flow of the system is illustrated in the figure 1.

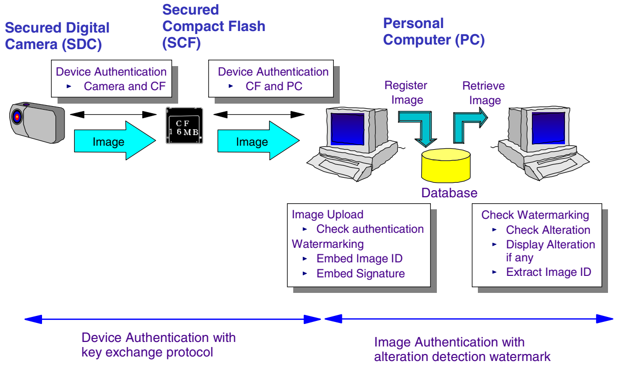
Secured Digital Camera (SDC)
Secured Compact Flash (SCF)
Personal Computer (PC)
Device Authentication ▸ Camera and CF
Device Authentication ▸ CF and PC
Register Image
Retrieve Image
Image
CF 16MB
Image
Database
Image Upload ▸ Check authentication
Watermarking ▸ Embed Image ID ▸ Embed Signature
Check Watermarking ▸ Check Alteration ▸ Display Alteration if any ▸ Extract Image ID
Device Authentication with key exchange protocol
Image Authentication with alteration detection watermark

Figure 1. System Overview of SIMON

Device Authentication

For this purpose we modified firmware inside a digital camera and a CompactFlash (CF) memory to create and defined an authentication protocol between the customized digital camera (SDC) and the customized CompactFlash (SCF) memory card. Similarly, we created another authenticcation chain between the SCF memory and the host PC (SPC) using a tamper-proof software module built into the device driver of the PC. This authentication chain will serve as a fully tamper-proofed transmission chain from the SDC to the SPC.

The authentication key used between the SDC and the SCF are set by the SDC manufacturer, and the authentication key used between the SCF and the PC is set by the insurance company, who are the user of this authentication chain. Therefore, each key is retained within each group and a symmetric key algorithm is sufficient for the implementation of device authentication.

While writing the content into the SCF, the SCF attaches a sector flag (SF) showing the success or failure in authenticating the SDC. This flag is inserted in each memory sector of the stored image data area to prevent the device swapping attack. Note that the SCF does not prohibit writing even the content is not authorized. It just adds an authentication when the contents are written with specific authentication to be recognized. The application system on the PC is written to only accept photos that come with properly authenticated flags. While reading the photo data from the ordinary CF memory device, or the SCF without proper authentication key, the application will treat the photos from this memory device as a “unknown source” and the photo will be indicated as a “source unknown” data. If the device authentication is completed, and the sector flag (SF) in the SCF does not present, the photo will be indicated as an “unauthenticated” data. If both the device authentication and the SF are properly verified, the application system then applies an invisible watermarking to the photo and stores it to the photo management database.

This authentication chain provides a handy and secure photo transmission method with relatively light additional overhead to the existing devices. However, the chain relies on a special memory device (SCF) which requires modification of the interface specification.

Hybrid Watermark System

In this prototype system, we use a hybrid type watermark for two different purposes. One is to carry an invisible digital signature and the content identification code for the verification of the integrity of the image and the other is to convey a pre-defined hidden structure to the detector, that can be used to identify the specific portion in the image that has been modified. We call this hybrid watermark system as Tamper-Detection Watermark (TDWM). With these two features, we can not only verify the integrity of the image, but also point out the specific part in the image that has been altered.

The watermark embedding process can be directly applied to the JPEG format image, and does not require JPEG de-compression. Therefore, it can be implemented into devices such as digital camera, which has a resource limitation.

The embedding is done by slightly manipulate the DCT coefficients in each of the sub-blocks of the image. The level of modification is controlled by a built-in visual model, in order to maintain the image quality of to the watermarked image. The embedding payload is generated by using a set of watermark key, embedding information and pseudo-random number generator, and modulated into the embedding pattern structure. The watermark is embedded all over the image area, redundantly, and the detection is based on a statistical analysis of accumulated and compiled small changes from each of the sub-blocks, therefore it can survive lossy transformation caused by JPEG decompression, re-compression and color space conversion. Noted that the JPEG decompression is also an information-losing process because of the following errors: the truncation error of pixel values in the conversion from the YCbCr color space to the RGB color space and the rounding error converting from floating point numbers to integers in the inversion step of the DCT. Therefore, for survivability we use pre-processing[3] of the DCT coefficients before watermarking. For example, we adjust the DCT coefficients to be in the range where truncation error does not take place in the conversion of the color space and limit the values of the quantized DCT coefficients so that they are sufficiently separated from each other so rounding error is negligible.

The embedded digital signature is a hashed summary of the JPEG-compressed image. Therefore, when we verify the JPEG decompressed image, the system automatically reproduces the original JPEG-decompressed image by estimating the quantization steps used in the JPEG compression from frequency analysis[3] of the DCT coefficients. The abovementioned preprocessing in the process of watermark embedding enables this reproduction.

The TDWM is used for two purposes. First, the TDWM is used as a secure and robust data channel to carry an invisible camera ID, time stamp and user ID as a "Photo ID" within the photo itself for content identification. Second, the TDWM is used to carry an alteration-sensitive structure for the identification of the location where alteration took place.[4] The TDWM is literally "woven" into the image data itself, and integrated with the content. The verification program distinguishes intentional alteration from normal artifacts created by JPEG compression. In order to create a forged photo, a forger would first need to compromise the watermark key, but would also need to conduct careful and complex image processing to satisfy both the cryptographic security as well as the check of the image structure.

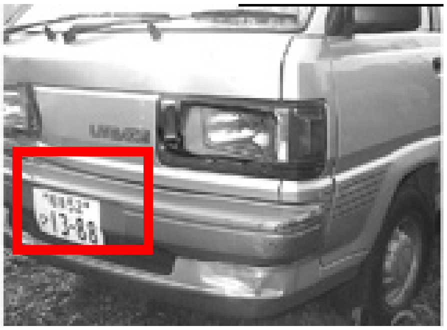

Figure 2. An altered location as identified by the TDWM

New Application Framework using Public Key Algorithm

SIMON took an orthodox device authentication approach, which is a solid and well-defined approach. However, this approach requires all of the devices in the transmission chain to fully compliant with a fixed single authentication specification. In the future e-business environment, this may not be the best approach, since the same content is more likely to be used in more than one platforms, environments and applications. Moreover, the technology, hardware, and service are changing rapidly, and it is not wise to obsolete the existing legacy system and other assets, each time a new application is introduced. One of the alternative solutions is to make the content as a self-contained authentication content, and separate the content authentication from the device (channel) authentication.

Framework of the System

The new proposal is to combine public key cryptography and watermark technology to create an end-to-end solution for the content. The solution covers the image-capturing device, such as digital camera or scanners, to the back end database of the enterprise application systems that use photos.

Firstly, the image-capturing device will generate a digital signature of the content using a built-in secret key inside the device, while the image is created. This secret key is buried in the hardware, or using a secure protocol to feed into the device by the user. The digital signature will be attached to the user data area of the content following the standard file specification of each format. The user can retrieve the attached digital signature, and using the public key, which is publicized by the originator of the image (or device manufacturer), to verify the integrity of the content.

The user of the photo can use the public key of the signed content to verify the integrity, and use the watermark ID to confirm the origin of the content. The digital signature can also be made as a proprietary signature by transmitting a unique secret key from the user to the designated camera to be used to sign the specific photos.

Advantages

In the proposed framework, multiple application systems can share a single hardware device and create proprietary image authentication processes by issuing their own “Wk”s. Thus, each insurance company can create and control its own watermarks and verify the integrity of the process with many repair shop owners. The digital camera manufacturer will only be a provider of the “tool”— they are not involved in the actual day-by-day photo transactions between the users of the camera and the inspectors of the images. The business solution developers will have to develop a random key generator to generate watermark keys, and provide secure storage for the keys as part of the application using the watermark extraction for integrity verification.

Implementation in Digital Cameras

Currently, many consumer digital cameras perform sophisticated image processing, enhancement and compression using software based platform. The additional computation processes required in the camera for the proposed system are watermark embedding and a one-way hash function. Both can be implemented as a streaming process that can be applied to the compressed image data stream. Therefore, it can be incorporated into the current architecture in the digital camera, and should not exceed the computational capabilities of today’s digital cameras. The pubic key decryption will only take place at the initialization of the photo taking session, therefore does not affect the response time while taking photos.

Dynamic Integrated Public Key DB

The enhancement of the system includes a service to collect, maintain and update the public keys used for verification of the images. The database of public key will be dynamically updated as a new public key is generated and publicized. Similarly, if the old key that are obsolete or removed, this will also be reflected to the database. User of the verification system will have to identify itself, register the key that are in use, and subscribe for the dynamic update service to keep their own local key database fresh.

Conclusion

We have designed a trusted photo exchange framework based on a content oriented approach, by combining with cryptographic digital signature and a newly developed hybrid watermarking technology. With this framework, the user of the photo can verify the origin and the integrity of the photo anywhere, without worrying the compatibility of the device, specification or the format of the images. The openness of the system, using the public key algorithm, enable third party to verify the photo, so that people can rely on what they see as a digital data. We will have to promote this as an open framework to the system integrators, as well as the device manufacturers for all of the users to enjoy the true benefit of the digital communication.

References

1. K. Toyokawa, N. Morimoto, S. Tonegawa, K. Kamijoh and A. Koide, *Secure Digital Photograph Handling with Watermarking Technique in Insurance Claim Process*, SPIE, International Conf. On Security and Watermarking of Multimedia Contents II, vol. 3971, No. 42, EI, (2000).
2. S. Shimizu, M. Numao, N. Morimoto, A method for identifying digital camera and detecting alteration on digital images, USP6005936.

Biography

Norishige Morimoto received his B.S. degree in Electrical Engineering from Keio University at Tokyo, Japan in 1987, and his M.S. degree in EECS from Massachusetts Institute of Technology at Cambridge in 1995. He joined IBM Japan in 1987, and worked on digital watermarking and rights management technology at the Tokyo Research Laboratory at IBM Japan since 1995. His work has primarily focused on the digital watermarking technology, image authentication and content management solutions.