Multimedia authentication for copyright protection

Mingsheng Yin

International School Beijing University of Posts and Telecommunications, Beijing, 100878, China

Abstract. Multimedia contents are easy to be copied and modified, so it is important to use authentication technology to ensure reliability and copyright security. Multimedia authentication technology is usually divided into digital signature and digital watermarking. In this paper, we introduce some basic image and video authentication technology, such as PCA algorithm and image signature method based on DCT coefficient, LSB -based digital image watermark, SVD-based digital image watermark, and video watermark. Through these digital content security technology, digital contents can be ensured security

1 Introduction

With the development of network technology, people can conveniently enjoy more and more digital multimedia contents. And users can easily edit and modify the digital contents with a large number of multimedia software. But the modified characteristics of digital products reduce their credibility. Therefore, it is necessary to verify the authenticity and integrity of multimedia contents.

Authentication, which can ensure reliability of the communication identity, content and process, is an important aspect of multimedia content security technology. So authentication is widely used in the network business systems, that provide multimedia content service, such as e-commerce, e-government, network copyright, etc.

Multimedia authentication technology is a new information security technology, which can prove whether the source of digital products is legal, and whether the content of digital products is reliable. Multimedia authentication technology is usually divided into two categories: digital signature and digital watermarking [1]. Digital signature is a kind of non-repudiation and encrypted information summary, extracted from original data. Then the digital signature information is usually stored as separate files and attached to the original data to verify the integrity and originality of the data. Digital watermarking is defined as the process of embedding special identification information directly into digital multimedia, such as digital image, audio, video, document, software and so on. Meanwhile, the watermark information can not affect the value in use of the digital media. Moreover, it is difficult to detect, distort or remove the digital watermarking. So, the watermark is used for verifying the copyright of the digital media content, authenticating the truth of the digital contents, and confirming the tracking infringement of the digital contents.

Digital signature and digital watermarking can be integrated in Digital Rights Management (DRM), which is treated as one of the most widely used multimedia authentication technology. And DRM can protect the intellectual property rights of all kinds of digital content, and to ensure the legitimate use of digital content throughout the life cycle, and also to balance the interests and needs of the various roles in the digital content value chain.

In our work, we will introduce the authentication technology, containing digital signature and digital watermarking. In part 2, digital signature is introduced, containing digital signature based on PCA algorithm and image signature method based on DCT coefficient. In part 3, digit watermark is introduced, containing the basic scheme, classification of digital watermark, LSB -based digital image watermark, SVD-based digital image watermark, and video watermark. In part 4, concludes our research.

2 Digital signature

Multimedia digital signature is useful for protection of intellectual property rights. It is perceptual features or short summaries of a multimedia object. The procedure of its extraction or generation is similar to conventional cryptographic hash functions: mapping a multimedia object of arbitrary size to short binary strings based on the response of the human visual/auditory system (HVS/HAS) to the input signal. Consequently, perceptually similar objects yield to similar signatures, while perceptually different objects different signatures. Hence, we call the procedure multimedia hashing [2].

2.1 Image digital signature

Since multimedia contains a lot of data, it is difficult and unrealistic to analyze the image directly. The purpose of image digital signature is to detect whether the image has been tampered with. According to the different ways of generating signatures, image authentication technology is mainly divided into complete authentication and content authentication. Complete authentication focuses on the entirety of the image data, and do not allow the slightest modification of image content. Digital signature technology uses hash function to generate the fixed size of the summary, and uses key encryption to generate signature. Then the signature is viewed as a watermark embedded in the original image or as binding additional information with the original image transmission. Content authentication generates signatures by extracting the features of the image, such as edge features. According to the similarity of the features, the image is judged to be maliciously tampered with, and the location of tampering is judged according to the position of the different features [3].

2.1.1 A general method of digital signature based on PCA (Principal Component Analysis)

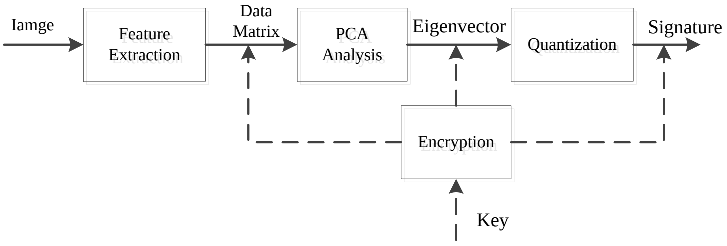

Figure 1. the architecture of the image digital signature

The architecture of the image digital signature is shown in Figure 1. Firstly, the features are extracted from the input images. The features can reflect the content of the image, such as the edge of the image, and the DCT low frequency coefficient. Then, these features comprise to a data matrix to represent the input images. Secondly, PCA analysis is performed to obtain an eigenvector matrix as an intermediate signature. Thirdly, every element (real number) in the eigenvector matrix is quantized into a byte integer in the range of 0 to 255, which is used as the final signature. Meanwhile, encryption algorithm is used with the keys to encrypt to protect the data security, containing the feature matrix, the eigenvector matrix and the signature.

2.1.2 Image signature method based on DCT coefficient. In the DCT transform domain, the low frequency component contains the main information of the image in the region, and it is also the most sensitive part of human visual information. In the DCT coefficient, the more the low frequency communication (AC) coefficients are selected, the stronger the difference of the image will get. The less the low AC coefficients are selected, the stronger robustness of the image you will get. Therefore, in order to get better difference and robust, DC coefficients and the first 7 low frequency AC coefficients of each block are selected. These coefficients comprise a DCT data matrix. Then PCA analysis is used to work on matrix, and its eigenvectors are used as the signature of the image. In order to make the signature length as short as possible, we need to quantify the eigenvectors. Considering the security of the signature, we also need to encrypt the quantized feature vectors, then we can get the final signature of the encrypted eigenvector as the final signature of the image [4].

3 Digital watermark

Digital watermark is a branch of information hiding. Digital watermark technology embeds the identification information into digital media, and does not affect the value of the original carrier. The digital watermark is not easy to detect and modify, but it can be recognized and identified by the manufacturers. Through the information hidden in the carrier, we can achieve the purpose of confirming the content creators/buyers, send confidential information, or judge whether the carrier tampered with. Digital watermarking is also an effective way to protect information security and achieve security traceability [5].

3.1 Basic of digital watermark

The target of digital watermark is to add the specific information to the media to protect the multimedia. The added information usually illustrates the copyright of the content. So, the digital watermark can protect the media from damaging and modifying easily. The universal model of watermark’s embedding and extracting are as following:

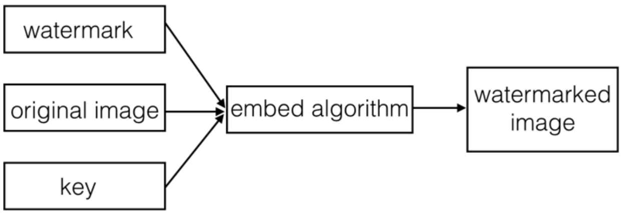

Figure 2. The process of embedding the watermark.

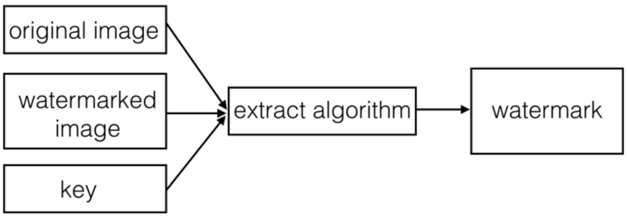

Figure 3. The process of extracting the watermark.

Figure 2 depicts the process of embedding the watermark, and Figure 3 depicts the process of extracting the watermark. The key in the figures are not a necessary input. But with the key existing the watermark can be more secluded and more resistant against attacks. According to the different usages, some of the embedded watermarks need to be recovered, while others need to be verified its existence. The former needs the watermark extracting algorithms while the latter needs watermark detecting algorithms. The process of embedment or extraction can be different in accordance with the specific algorithm it used.

3.2 Classification of digital watermark

Digital watermark can be divided into a variety of categories from many different angles [6].

Robust watermark / fragile watermark: Robust watermark is mainly used to identify the copyright information of the digital media. It requires the embedded watermark to resist normal edit and malicious attacks. And it means that it would not be damaged in large scale after being rotated, cut, and compressed. Fragile is opposite to the robust watermark. Just as its name, fragile watermark is sensitive. It can be used to detect whether the original information is modified.

Image watermark / audio watermark / video watermark / text watermark: This kind of classification is defined by the carrier of the watermark. In last part, we research on the image watermark.

Spatial domain watermark / frequency domain watermark / time domain watermark / temporal domain watermark: This kind of classification is defined by the location where the watermark is concealed. Original data is normally being presented on spatial domains or time domains, and it can be cast to other domains when the signal is handled by different signal managements. Every single domain can be embedded with digital watermark, so that this definition comes out by the domains.

Invisible watermark / visible watermark: Visible watermark is just an identifier that covers on the original image, similar to the paper watermark. This also means that this kind of watermark can be noticed optically. On the contrary, invisible watermark is the one that cannot be recognized optically. Invisible watermark is more widely used.

3.3 A simple case: Spatial domain LSB watermark

The least significant bit algorithm (LSB) is a typical spatial domain information hiding algorithm. The LSB algorithm uses a specific key to generate a random signal through the m sequence generator, and then is arranged into 2-dimensional watermark signal, based on a certain rule. The watermark signal is hidden in the lowest position, which is equivalent to a weak signal, so it is difficult to detect in the sense of vision and hearing. The detection of LSB watermark is realized by the correlation calculation of the image. The LSB algorithm can hide more information, but the robustness is poor. However, LSB still plays a very important role in the covert communication.

3.4 A More Complicated Case: SVD-based digital image watermarking:

3.4.1 The singular value decomposition. Singular Value Decomposition (SVD) is one of effective numerical analysis tools used to analyze matrices. In SVD transformation, a matrix can be decomposed into three matrices, which have the same size. Given a real matrix A ($n\times n$), this matrix can be transformed into three components, U, D and V respectively, such that:

$$
\begin{aligned}
[U \quad D \quad V] &= \mathrm{SVD}(A), \quad A' = UDV^{\mathrm{T}} \\
&= \begin{bmatrix} \boldsymbol{u}_{1,1},\ldots,\boldsymbol{u}_{1,n} \\ \boldsymbol{u}_{2,1},\ldots,\boldsymbol{u}_{2,n} \\ \vdots \\ \boldsymbol{u}_{n,1},\ldots,\boldsymbol{u}_{n,n} \end{bmatrix}
\begin{bmatrix} \boldsymbol{\sigma}_{1,1},0,\ldots,0 \\ 0,\boldsymbol{\sigma}_{2,2},\ldots,0 \\ \vdots \\ 0,0,\ldots,\boldsymbol{\sigma}_{n,n} \end{bmatrix}
\begin{bmatrix} \boldsymbol{v}_{1,1},\ldots,\boldsymbol{v}_{1,n} \\ \boldsymbol{v}_{2,1},\ldots,\boldsymbol{v}_{2,n} \\ \vdots \\ \boldsymbol{v}_{n,1},\ldots,\boldsymbol{v}_{n,n} \end{bmatrix}^{\mathrm{T}} \\
&= \sum_{i=1}^{n} \boldsymbol{\sigma}_i \boldsymbol{u}_i \boldsymbol{v}_i^{\mathrm{T}},
\end{aligned}
$$

where the U and V components are $n \times n$ real unitary matrices with small singular values, and the D component is an $n \times n$ diagonal matrix with larger singular value entries [7].

SVD used in digital image processing has some advantages. Firstly, the size of the matrices from SVD transformation is not fixed and can be a square or a rectangle. Secondly, singular values in a digital image are less affected if general image processing is performed. Thirdly, singular values contain intrinsic algebraic image properties.

3.4.2 SVD-based watermarking. In the embedding procedure of digital watermark, the largest coefficients in D component are modified and used to embed a watermark. The modification is determined by the quantization mechanism. After that, the inverse of the SVD transformation is performed to reconstruct the watermarked image. Because the largest coefficients in the D component can resist general image processing, the embedded watermark is not greatly affected. Also, the quality of the watermarked image can be determined by the quantization. Thus, the quality of the watermarked image quality can be maintained [8].

To extract an embedded watermark, the SVD transformation is employed and the largest coefficients in the D component are examined. After that, the watermark is extracted. The watermark embedding and extracting procedures can be described as follows.

The watermark embedding procedure:

Step 1. Partitioning the image into blocks.

Step 2. Performing SVD transformation.

Step 3. Extracting the largest coefficient $D(1,1)$ from each D component, and quantizing it by using a predefined quantization coefficient Q. Let $Z = D(1,1) \bmod Q$.

Step 4. Embedded watermark bit is valued to 0, if $Z < 3Q/4$, $D(1,1)$ modify to $D^{'}(1,1) = D(1,1) + Q/4 - Z$. Otherwise, $D^{'}(1,1) = D(1,1) + 5Q/4 - Z$.

Step 5. Embedded watermark bit is valued to 1, if $Z < Q/4$, $D(1,1)$ modify to $D^{'}(1,1) = D(1,1) - Q/4 + Z$. Otherwise, $D^{'}(1,1) = D(1,1) + 3Q/4 - Z$.

Step 6. Performing the inverse of the SVD transformation to reconstruct the watermarked image.

The watermark extracting procedure:

Step 1. Partitioning the watermarked image into blocks.

Step 2. Performing SVD transformation.

Step 3. Extracting the largest coefficient $D^{'}(1,1)$ from each D component and quantize it by using the predefined quantization coefficient Q. Let Z = $D^{'}(1,1)$ mod Q.

Step 4. If $Z < Q/2$, the extracted watermark has a bit value of 0. Otherwise, the extracted watermark has a bit value of 1.

In this scheme, the steady property of the largest D component coefficients resisting the image processing was preserved. However, the D component is a diagonal matrix, in which only a small number of the coefficients could be used. In addition, the modification of the largest coefficients would cause a greater measure of image degradation.

3.5 Video watermark

Since video data is mostly transmitted and stored in compressed format. Therefore, video watermarking algorithms are combined with coding system to achieve its value. Video watermarks can be roughly divided into three different watermark embedding schemes: pre-built embedded, built-in embedded and post-embedded scheme. So, there are three different extraction schemes: pre-built extraction, built-in extraction and post extraction scheme. Three different embedding and extracting programs are correspond to different stages of specific video coding system. Watermark extraction program should be based on the design of watermark embedding scheme. Pre-extraction programs generally correspond to post embedding scheme, which is carried out by analyzing the video stream compression. Built-in extraction corresponds to the built-in embedding by partially decoding information of the video stream to extract the watermark information extraction program, which is then set to complete the watermark extracted from the reconstructed video sequence information, and identification, corresponding to the pre-embedded. Figure 4 shows the video watermarking schemes [9].

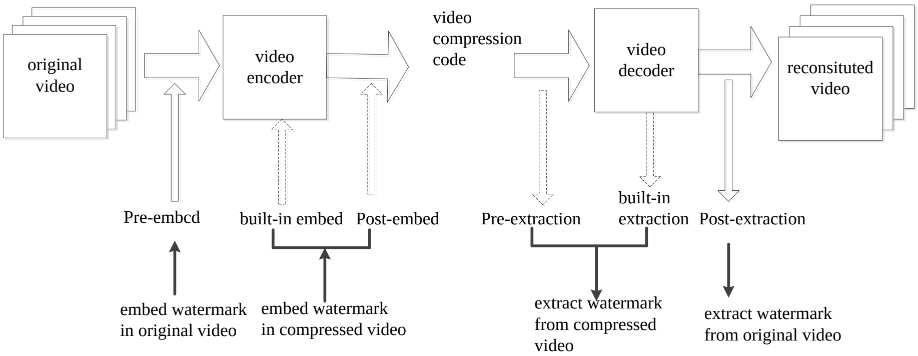

Figure 4. Schemes of Video Watermarking

4 Conclusion

With the popularity of digital products, multimedia authentication technology will have more broad application prospects, and play an increasingly important role in forensic, electronic commerce, network copyright, press releases etc. The future of multimedia authentication technology should be developed as follows: (1) Signature technology and digital watermarking technology are integrated. (2) The signature or watermarking algorithms have repairing abilities. (3) The signature or watermarking algorithms have multiple effects.

References

[1] Wu C W. On the design of content-based multimedia authentication systems[J]. IEEE Transactions on Multimedia, 2002, 4(3): 385-393.

[2] Dittmann J, Steinmetz A, Steinmetz R. Content-based digital signature for motion pictures authentication and content-fragile watermarking[C]//Multimedia Computing and Systems, 1999. IEEE International Conference on. IEEE, 1999, 2: 209-213.

[3] Lin C Y, Chang S F. Generating robust digital signature for image/video authentication[C]//Multimedia and Security Workshop at ACM Multimedia. 1998, 98: 49-54.

[4] Piva A, Barni M, Bartolini F, et al. DCT-based watermark recovering without resorting to the uncorrupted original image[C]//Image Processing, 1997. Proceedings., International Conference on. IEEE, 1997, 1: 520-523.

[5] Van Schyndel R G, Tirkel A Z, Osborne C F. A digital watermark[C]//Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference. IEEE, 1994, 2: 86-90.

[6] Saini L K, Shrivastava V. A survey of digital watermarking techniques and its applications[J]. arXiv preprint arXiv:1407.4735, 2014.

[7] Chandra D V S. Digital image watermarking using singular value decomposition[C]//Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on. IEEE, 2002, 3: III-III.

[8] Chang C C, Tsai P, Lin C C. SVD-based digital image watermarking scheme[J]. Pattern Recognition Letters, 2005, 26(10): 1577-1586.

[9] Zhang J, Li J, Zhang L. Video watermark technique in motion vector[C]//Computer Graphics and Image Processing, 2001 Proceedings of XIV Brazilian Symposium on. IEEE, 2001: 179-182.