Lutz Vorwerk, Frank Losemann, Christoph Meinel :
Suggestion for an Alternative of watermarking and digital Signatures
in Proceedings of SPIE Conference on Photonics West (PhotonicsWest 2001), vol. 4314, SPIE Press, San Jose, California, USA, pp. 158-165, 1, 2001.

Suggestion for an alternative of watermarking and digital signatures

L. Vorwerk, F. Losemann, Ch. Meinel
Institute of Telematics, Trier, Germany

ABSTRACT

Watermarking consists of hiding of information within a multimedia element such as an image, a text, music or a video clip. Hiding information within other information is called steganography. A TV station's logo may serve as an example for perceptible information. Steganographical methods are needed to integrate non-perceptible information: that means this information is hidden within a multimedia element like an image.

Common operations like rotating, scaling, smoothing, sharpening, clipping, lossy compression or integration of hissing can destroy watermarks. The protection of a copyright on multimedia elements is one of the main uses of digital watermarks. All hidden information is protected by digital signatures which use an asymmetric key-pair to ensure security. The signed information is then integrated into the multimedia element as a non perceptible-digital watermark. A digital watermark is not sufficient for this task.

In the presentation, the case of a preexistent database which contains objects describing the owner of a multimedia element and image's features will be examined. A trusted party adds this information to an entry in its database and performs a hash over the data of the multimedia element. Additional operations will be performed to extract the main features of the multimedia element.

INTRODUCTION

Watermarking comprises hiding of information within a multimedia element such as an image, a text, music or a video clip. Hiding information within other information is called steganography. In the context of watermarking, one of the first steps to take is the decision between the integration of perceptible and non-perceptible information. The TV station's logo may serve as an example for perceptible information. It is openly shown on the screen during an entire movie. Non-perceptible information uses steganographical methods: This information is hidden within the multimedia element. The ulterior motive is the transfer of hidden information within other information. Invisible ink is one of the best-known examples. In the following, we consider the case of digital images only.

A crypto analyst (i.e. a hacker) may try to find such hidden information or even try to remove it from a digitally watermarked image. After removing the digital watermark, he or she will try to add a different digital watermark in order to change the copyright illegally. Common operations like rotating, scaling, smoothing, sharpening, clipping, lossy compression or integration of hissing can destroy watermarks. There are several methods to make watermarks resistant against such operations, but these methods do neither cover all operations nor all multimedia elements.

The protection of copyright of multimedia elements is one of the main uses of digital watermarks. All hidden information is protected by digital signatures which use an asymmetric key-pair to ensure security. The pair consists of one private key, which is only known to the signer, and one public key which has been distributed to all recipients who want to verify the signature. The information which has to be signed is first hashed and then encrypted by the signer's private key. Figure 1 gives an overview of this process which is described in the following section in more detail. The signed information is then integrated into the multimedia element as a non perceptible-digital watermark.

A mechanism is needed to protect copyright and to prevent attacks like removing or replacing copyright. A digital watermark is not sufficient for this task. Let us examine the case of a preexistent database which contains objects describing the owner of a multimedia element and image's features. This database is managed by a third trusted party which guarantees protection of all information it obtains. The following scenario describes the procedures for obtaining copyright of a multimedia element: A customer constructs a request for a multimedia element in addition to a description of that

multimedia element and transmits it to the trusted party through a secure connection such as a secure socket layer (SSL)[1] or a transport layer security (TLS)[2]. For the request, a certificate is used that contains the requestor's entire information. The

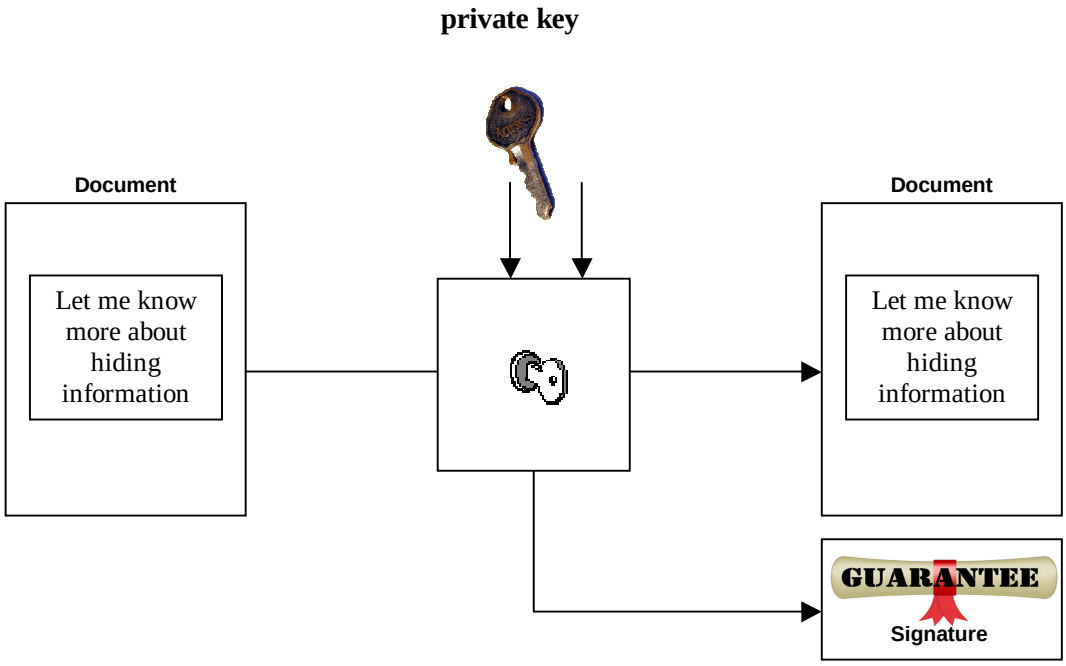

Figure 1: The process of digitally signing data

trusted party adds this information to an entry in its database and performs a hash over the data of the multimedia element. Additional operations will be performed to extract the main features of the multimedia element. In the case of images, this can be done by operations like dilatation and erosion which are often used in pattern recognition. The descriptions have to be stored in the database in a structured form.

SECURITY ASPECTS BY USING WATERMARKS

Nowadays, the increasing development of internet applications for the transfer of private medical data forces a need of high secure mechanisms that protect the data to be transferred over the internet as well as infrastructures especially developed to provide authentication and authorization mechanisms. In the area of telemedicine such mechanisms are important for the transfer of data like digital prescriptions, image management and processing of patient data.

In this regard public key infrastructures are used to assign the public key of a user with owner information. The public key together with the owner information represents a certificate. Certificates are managed in a certificate database, which provides services like certificate verification, request, enrollment and management. This certificate database is located in a Trust Center, that acts as a trusted third party, provides certificates and provide services like certificate verification. The private key is kept by the owner preferably on a chip card. The private key can not reconstructed from the public key, but the public key can be reconstructed by using the private key. That is because this kind of key pair is called asymmetric. Here a first check is done if the public key belongs to the private key.

The process of authentication is the most important process in a PKI[3], because the verification of person ID is a process, that decides what access rights assigned to this person and if a person is allowed to use components of the PKI.

This section describes some aspects that are necessary to understand what security means when transferring data from one destination to another. There are different possibilities to protect data from third persons who want to read this data.

One way is to hide the data in other data. This concept is called steganography and is used for example in digital watermarking where data that belongs to an owner of an image is integrated in the image and protected against modification by using a digital signature.

A digital signature of a message is a sequence of digits computed by using a secret known only to the signer (private key), and the content of the message being signed (building a hash). Signatures must be verifiable; if a dispute arises as to whether a party signed a document a trusted third party should be able to resolve the matter equitably, without requiring access to the signer's secret information. Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation. One of the most significant applications of digital signatures is the certification of public keys in large networks. Certification is a means for a trusted third party (TTP) to bind the identity of a user to a public key, so that at some later time, other entities can authenticate a public key without assistance from a trusted third party. The concept and utility of a digital signature was recognized several years before any practical realization was available. The first method discovered was the RSA signature scheme, which remains today one of the most practical and versatile techniques available. Sub-sequent research has resulted in many alternative digital signature techniques. Some offer significant advantages in terms of functionality and implementation. Figure 2 gives an illustration of how a trusted third party may verifies a digitally signed piece of data.

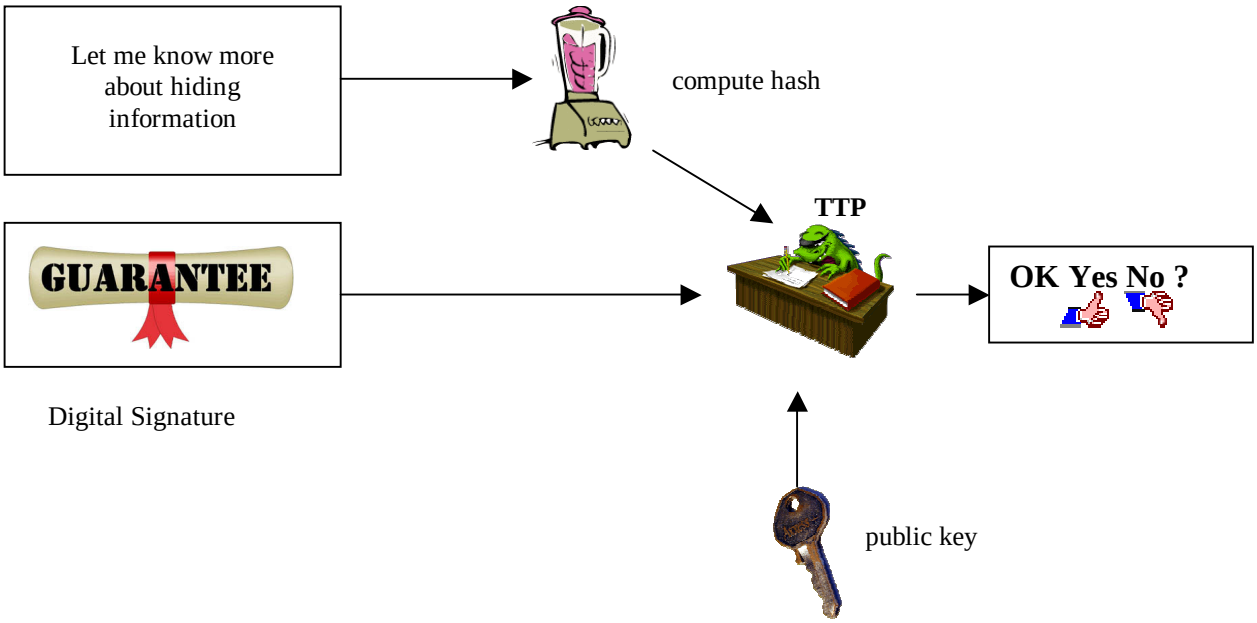

Figure 2: Verification of a digital signature by a trusted third party (TTP)

A digital signature builds a hash over the data that has to be signed. The hash is an encryption that is not reversible. The hash is encrypted with a private key. The private key is a secret key that can only be assigned to one and only one public key. The public key serves as a helping tool to exchange data with the owner of the assigned private key. To verify a digital signature, the hash is first decrypted with the public key and then it is checked whether the decrypted data (hash) matches the hash that has been generated by the data to verify if the data is changed.

Some reasons to use a digital is signatures will be described next. One is evidence. In this context a signature is used to assign a person to the signed data in that way that the person owns this data. This kind of signature can be regarded as a "personal touch" applied on the a piece data. A piece of data can also be signed for the reason of Ceremony. This feature is evoked by a person who want to let to know other persons from the receipt of the data. The wish to mark the piece of data with simply a signature or a signed comment serves as an example for Ceremony. A signature can serve as a ticket which authorize or legalize an action. This is often called an approval. Another aspect in which digital signatures will be used are transactions. The digital signature is used to sign a transfer. This happens automatically and improves therefore the speed of such actions by using digitally signed rules for the transfer.

The described reasons for the usage of digital signatures there are some preconditions that must be fulfilled. One is called signer authentication. Here, the fact that a signature must identify a person and is difficult to produce without authorization is important.

A signature must identify what is signed. This information must not be falsified or altered without notifying to authentize a piece of data. It must be possible to mark an event, indicate approval and authorization, and establish the sense of having legally consummated a transaction with a signature to perform an affirmative act.

The creation, verification of a signature and the signature itself must provide the greatest possible assurance of authenticity and validity with the least possible expenditure of resources.

The preconditions described above allows to proof if the examined data are original or delivered correctly to protect both sender and receiver against false denials.

Another way is to encrypt the data. That means to protect the data against modification and against information retrieval. The first step of such a method is the generation of a key. An algorithm patented in the USA which has been declared 'secure' is Rivest Shamir Adleman (RSA). This algorithm is based on the problem of factoring large integers.

Another method is that of Diffi and Hellman. The algorithm computes discrete logarithms modulo a prime number. The renewal of patent will be processed by developing a health professional card[4].

A third method is that of using elliptic curves to compute the keys. The keys are shorter than in RSA and evoke, therefore, a smaller bandwidth and memory requirements.

With the key generation, a key pair is created: the public and the private key. The public key is now used to encrypt the data that can now only be decrypted by the owner of the private key. This method is called 'asymmetric encryption' because of the fact that one key is used for encryption and another one is used for decryption. Another method is called symmetric encryption. This method use one key to encrypt and decrypt the data. It is less time-consuming but also less secure because the key can get deciphered by a crypto-analyst.

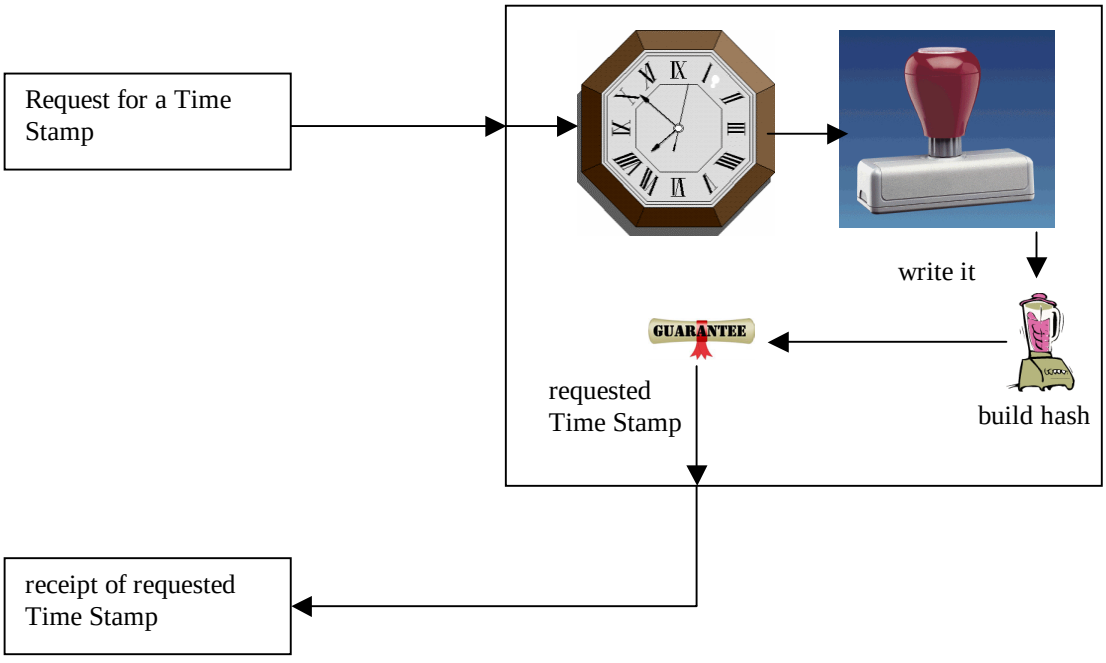

Figure 3: The creation of a requested time stamp by a time stamping service (TTS).

TIME STAMPING

To the data like a text or an image the time of its creation is attached. This feature serves the verification at which time the data is created. The time stamp serves to identify for example misusage of digital signatures. If a document was signed including a timestamp and a misusage is detected then a revocation can be performed that make all documents with time stamps after the original document invalid and therefore untrustworthy. Examples where time stamping is used are the file transfer protocol (FTP) and hypertext transfer protocol (HTTP).

A time-stamping service (TSS) is a collection of methods and techniques providing long-term authentication of digital documents. The object of a TSS is to authenticate not just the document but also the moment in time at which the document is submitted for authentication. In figure 3 the process from the request of a time stamp to the receipt of the signed time stamp is illustrated. The first step is that a request occurred. Afterwards the time has to be determined. This usually is performed by getting global time. The time is written into a document that is afterwards signed and then send back to the requestor. the exchange of timestamps is usually performed on an encrypted connection to prevent attacks.

INTRODUCTION TO WATERMARKING

By using digital media, copies of these media can be made without loss of data and therefore quality. There is a great problem to guarantee copy rights and manipulation of digital data. The field of cryptography may be used to get out of this problem. Encryption is a part of the solution. It protects data only on the way from one point to another. In case of e.g. images the receiver wants to display the image and therefore have to decrypt it. Once encrypted the data may be manipulated or copied by the owner of the key or can be copied from an intruder from disk.

The use digital signatures for data that have to be protected against breaking of copy right is also a part of the solution. Signatures can be removed from the data and must be consistent against allowed manipulations like compression or in cases against altering. The problem is that there is no control about the manipulations that may be performed on those data. Thus, a solution may be found in the field of digital watermarking[5].

Digital watermarking adds hidden information to the data. This information is either perceptible or non perceptible and have to be resistant against manipulations, so that a removal of this data evokes a destruction of data that is copy righted. This new information must be encrypted by a private key in order to ensure that statistical and analytical attacks are prevented. Figure 4 shows a perceptible watermark.

Figure 4: Example of a watermark

KIND OF ATTACKS TO WATERMARKS

There are a lot of methods to try to remove or destroy digital watermarks. This section gives an overview of these methods. To make a watermark unreadable it is necessary to add noise to the data. This can be achieved by analog to digital and afterwards digital to analog converting of the data. Another method transform the data into waves and filter those waves which does not affect the semantic of the data. This method is applied e.g. to images and audio data. Alternatively, you can divide the data into pieces which are independent itself. For example you can crop an image. A watermark should survive

this. An often used method is to compress the data. In the area of image management often lossy image compression is used to save memory allocation. This procedure can affect watermarks. Another method in image management is to rotate or resize the image. This should be also kept in mention. Yet another attack is to estimate the watermark and then subtracting it from the data. Another attack is to add an own watermark. A reason to add timestamps to the watermark to easy the determination of the owner when more than one watermark occur. Harder attacks are to permute or super scrambling the data.

APPLICATIONS OF WATERMARKING

This section describes where watermarks are applied. Video and audio watermarking were discussed above. Hardware and software watermarking are valuable to protect software and logic circuits against unauthorized copying. It is interesting for the appliance of watermarks to hide labels in order to annotate objects. This method is called labeling. The advantage of this method is to integrate the owner information into the object to prevent cutting it out.

THE SUGGESTION

The alternative consists of a combination of existing methods to protect owner rights, watermarking techniques and pattern recognition. There are several approaches that combine digital signatures and watermarking by integrating encrypted information as watermarks in the data that must be watermarked. An example is the integration of individual data as a signature that identifies the person who is belonging to the data. Another example uses signed data that contains information of a patient and integrate this signature together with the data in a radiological image to have an assignment from image to patient. The signature and the data that belongs to the signature have to be encrypted. These concepts consider only the method to integrate information into other data. But, what is about a concept that deals with specific features of the data to be signed or watermarked. These features will be extracted from the data and will be later used to identify these data. These identifiers will be considered as a part of a certificate, that contains further information about the object. The identifier will be encrypted and therefore not readable for other persons.

The process of extraction of the features will be now described. The process is like pattern matching, which is used to divide the data into objects that have specific characteristics. In case of digital imaging the methods of erosion and dilatation will be used to detect such objects. If only data is considered, a method has to be created that build the object by using data not affected through loss less or lossy compression. To achieve this a method has to be developed that has a table of all effects of compression methods. When a pattern is chosen the table will be consulted to determine which data could be a part of this pattern.

During the process of estimation if data belongs to a certificate that contain an identifier, the identifier mostly does not match exactly to the computed identifier. So some conditions have to be considered that helps to verify if the data is in the scope of the identifier. The scope is an interval that is derived from the table of effects. An object that lies within such a scope is considered as a candidate that matches to this identifier.

A pattern match can be happened partially by cutting pieces out of the original data, for example in case of cutting or cropping an image or cutting sound data. In this case the splinter of data should be in the focus of matching candidates.

Considering the case of protection of Internet data to ensure the verification a human being (the owner) is informed by the pattern matching unit. The owner got a list of the data that is in the scope of his or her data. This happens in the following case. Assuming there is a database that contains the locations of legal copies of the data. If the location of the data does not match with the locations to which the data is send legal and the data is copyright protected.

In case of non-Internet use the verification of data is evoked by the suspicion of an illegal copy. In order to verify this object, the object has to be digitized. For example, in case of an image it has to be scanned in. The following process is identical to that one used in the case of protection of Internet data.

Considering the case of the transfer of digital radiological images the standard of digital imaging and communication of medical data (DICOM) influences a large variety of institutions and companies. In DICOM[4] the images are separated from the patient data. This feature is very good to increase the speed of image transfer and management. The image has not to be encrypted because the patient data itself may be encrypted to ensure the anonymity and privacy of the patient. This is the

reason why the image data can be send separately from patient data. There are many projects to integrate encryption and digital signatures in applications that deals with healthcare[6,7]. To follow the new concept described above, the features of the image will be transformed to an identifier. Afterwards, this identifier is stored in a suited attribute of a certificate and this certificate is managed in a trust center that provides the certificate for verification if the data belongs to the patient data contained in the certificate. Private patient data is not contained in the certificate. It is located in a database. The certificate has a link to the database. Only the person who has knowledge about the corresponding private key is authorized to access this data.

The theory can be extended to other scopes of application. In digital imaging exist many tools that can be very helpful to build identifiers over an image or a video or other data.

Additionally, the certificate which contains the identifier for a data object can be extended by an attribute that represents a link to a log database that manages changes of the data object which belongs to an identifier. The log data base contains to each modification a time stamp, the modification, and the new identifier.

Putting it all together we have the system that is shown in figure 5. A data object that is chosen for marking is send to a certified feature extractor through an encrypted connection. The feature extractor locates the characteristics of the data object to build the identifier. To ensure that attacks will be prevented the feature extractor is certified, that means the built extractor is signed by the feature extractor. The signed and afterwards encrypted identifier is sent to the a trusted third party located in a trust center that creates a certificate for this object. To the information of the certificate a link to a database is added that contains additional information and a log for modifications performed on this data. The information for the object and the first identifier are stored together with a time stamp which is obtained by a time stamping service.

To verify the object the identifier is build again by the feature extractor and compared with the newest identifier found in the database.

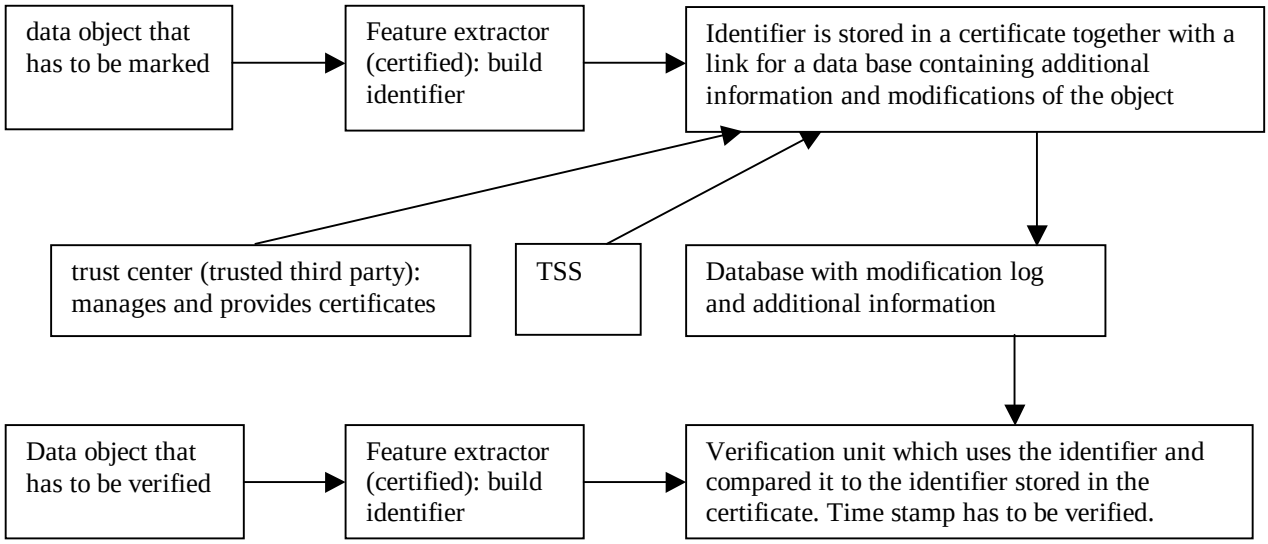

Figure 5: Process of marking and identification

CONCLUSION

The methods of extracting features have to be evaluated in more detail. This Paper described an suggestion for alternative of watermarking and digital signatures. A good way to mark an object is to hide information within other information that is

called steganography. All hidden information is protected by digital signatures which use an asymmetric key-pair to ensure security. The signed information is then integrated into the multimedia element as a non perceptible-digital watermark. A trusted party adds this information to an entry in its database and performs a hash over the data of the multimedia element. The process of digitally signing data is one part that leads to the trusted party who adds this information to an entry in its database and performs a hash over the data of the multimedia element. In this regard public key infrastructures are used to assign the public key of a user with owner information. The public key together with the owner information represents a certificate. The private key can not reconstructed from the public key, but the public key can be reconstructed by using the private key. There are different possibilities to protect data from third persons who want to read this data. One way is to hide the data in other data. This concept is called steganography and is used for example in digital watermarking where data that belongs to an owner of an image is integrated in the image and protected against modification by using a digital signature. Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation. Verification of a digital signature happens by a trusted third party (TTP).

By using time stamping to the data like a text or an image the time of its creation is attached. This feature serves the verification at which time the data is created. The time stamp serves to identify for example misusage of digital signatures. There is a great problem to guarantee copy rights and manipulation of digital data. Digital watermarking adds hidden information to the data. There are several approaches that combine digital signatures and watermarking by integrating encrypted information as watermarks in the data that must be watermarked. An example is the integration of individual data as a signature that identifies the person who is belonging to the data. Another example uses signed data that contains information of a patient and integrate this signature together with the data in a radiological image to have an assignment from image to patient. The signature and the data that belongs to the signature have to be encrypted. These concepts consider only the method to integrate information into other data. If only data is considered, a method has to be created that build the object by using data not affected through loss less or lossy compression. A pattern match can be happened partially by cutting pieces out of the original data, for example in case of cutting or cropping an image or cutting sound data. The owner got a list of the data that is in the scope of his or her data. If the location of the data does not match with the locations to which the data is send legal and the data is copyright protected.

In DICOM the images are separated from the patient data. Afterwards, this identifier is stored in a suited attribute of a certificate and this certificate is managed in a trust center that provides the certificate for verification if the data belongs to the patient data contained in the certificate. Private patient data is not contained in the certificate. Only the person who has knowledge about the corresponding private key is authorized to access this data.

Additionally, the certificate which contains the identifier for a data object can be extended by an attribute that represents a link to a log database that manages changes of the data object which belongs to an identifier. The log data base contains to each modification a time stamp, the modification, and the new identifier.

The feature extractor locates the characteristics of the data object to build the identifier. To the information of the certificate a link to a database is added that contains additional information and a log for modifications performed on this data.

REFERENCES

1. Transport Layer Security Working Group, Dierk, T., Allen, Ch., 1997, The TLS-Protocol Version 1.0.
2. Handbook of Applied Cryptography, Alfred J.Menezes, Paul C. van Oorschot, Scott A. Vanstone.
3. TeleTrust Kryptoreport, Kryptographische Verfahren im Gesundheits- und Sozialwesen.
4. *Digital Imaging and Communications in Medicine*, Teil 1-6. NEMA Standards Publication PS3.X, 1996.
5. Information hiding techniques for steganography and digital watermarking, *Stefan Katzenbeisser, Fabien A. P.Petitcolas (Editors)* Artech House Books, 1999 ISBN 1-58053-035-4
6. Constructing a Secure HIPACS with structured reporting, L.Vorwerk, F. Losemann, C. Meinel, PACS Design and Evaluation: Engineering and Clinical Issues, G. J. Blaine, E. Siegel, San Diego, USA, 2000
7. security in health care: An overview, L. Vorwerk, Ch. Meinel, new aspects of high technology medicine, monduzzi editore, Hanover (Germany), 2000