Dittmann, Steinebach, Croce Ferri, Vielhauer, Steinmetz, Wohlmacher; Framework for media data and owner authentication based on cryptography, watermarking and biometric authentication . In: Multimedia Systems and Applications IV, August 21 - 22, Denver, USA, Proceedings of SPIE, Bellingham WA, USA, Tescher A., Vasudev B., Bove M. (Eds.), S. 198 - 209, ISBN 0-8194-4242-9, 2001

Framework for media data and owner authentication based on cryptography, watermarking and biometric authentication

J. Dittmann [a], M. Steinebach [a], L. Croce Ferri [a], C. Vielhauer [b], R. Steinmetz [b], Petra Wohlmacher [c]

[a] GMD - German National Research Center for Information Techology
IPSI – Integrated Publication and Information Systems Institute
Darmstadt, Germany
[b] Technical University Darmstadt and Platanista GmbH, Germany
[b] University of Klagenfurt, Austria

ABSTRACT

Protecting the media of the future - securing the future of the media is an essential task for our new century. Security is defined by security measures, e.g. confidentiality, integrity, authenticity, and non-repudiation. Most of these measures are using watermarking techniques and cryptographic mechanisms like cipher systems, digital signature schemes, and authentication protocols. The security of these mechanisms is mainly based on the authenticity of specific data like keys and attributes – both data must be dedicated to its owner in an authentic manner. Otherwise, the authenticity of data and of owners can not be guaranteed and subsequently, the security can not be assured. Therefore in our paper we want to focus on data and entity (owner) authentication. We introduce a general framework to protect media data by combining different existing techniques: cryptographic, watermarking and biometric approaches. As an example we describe general concepts for a content-fragile watermarking approach for digital images and a generic approach for biometric authentication.

Keywords: multimedia data security, watermarking, cryptography, biometrics

1. MOTIVATION

Since digital data can easily be copied, multiplied without information loss, and manipulated without any detection, security solutions are required, which encounter these threats. Security solutions are especially of interest for such fields as distributed production processes and electronic commerce, since their producers provide only access control mechanisms to prevent misuse and theft of material. Several catalogues for security criteria have been published [6]. These catalogues define security criteria within different classifications regarding basic threats. The following security requirements are essential for multimedia systems. These requirements can be met by the succeeding security measures:

- *Confidentiality:* Cipher systems are used to keep information secret from unauthorized entities.
- *Data authentication:* Message authentication codes, digital signatures, fragile digital watermarking, and robust digital watermarking enable the proof of origin. For data integrity the alteration of data can be detected by means of one-way hash functions, message authentication codes, digital signatures (especially content-based digital signatures), fragile digital watermarking, and robust digital watermarking.
- *Entity authentication:* Entities taking part in a communication can be proven by authentication protocols mainly based on three classes [24]: (i) possessions (what you have); (ii) knowledge (what you know); and, (iii) biometrics (unique personal traits). These protocols ensure that an entity is the one it claims to be.
- *Non-repudiation:* Non-repudiation mechanisms prove to involved parties and third parties whether or not a particular event occurred or a particular action happened. The event or action can be the generation of a message, the sending of a message, the receipt of a message and the submission or transport of a message. Non-repudiation certificates, non-repudiation tokens, and protocols establish the accountability of information. These mechanisms are based on message authentication codes or digital signatures combined with notary services, timestamping services and evidence recording.

The security measures mentioned above, use cryptographic mechanisms, digital watermarking or biometric based techniques. The security of these mechanisms is mainly based on the authenticity of specific data like keys and attributes – both data must be dedicated to its owner in an authentic manner. Otherwise, the authenticity of data and of owners can not be guaranteed and subsequently, the security can not be assured. Therefore in our paper we want to focus on data and entity (owner) authentication. The focus is also concentrated on the problems with multimedia data deriving from applying cryptographic mechanisms.

In the following sections, we introduce a framework designed in our project H2O4M – **Water**marking **for Media** (http://www.darmstadt.gmd.de/mobile/projects/h2o4m/) for data and owner authentication based on cryptography, watermarking and biometric authentication. H2O4M is a joint project of GMD-IPSI and the German broadcast archive DRA funded by the German government. The project's intention is to classify the different watermarking schemes, to find quality measures and to improve watermarking technologies. Beside the theoretical evaluation one major goal and so far the first of its kind is the integration of the watermarking algorithm into a content management system. Our paper starts with the definition of requirements in our sample scenario H2O4M. Section 3 introduces existing general solutions for owner and section 4 for data authentication. In section 5 we discuss our framework using the introduced security features for data and owner authentication. As an example we introduce a generic concept for biometric authentication and a content-fragile watermarking scheme for digital images. Finally we summarize our work and show future aspects.

2. REQUIREMTS IN THE EXAMPLE SCENARIO: H2O4M

In the H2O4M scenario the content provider German Radio Archive (Deutsches Rundfunkarchiv or DRA) offers a huge archive of images, video and audio data. Presently the DRA has no public access to the material, but future plans imply to open the archive to customers over the internet. The idea is to transmit the data to a content server with internet access and to offer a search engine to browse via the content management system through the archive. Figure 1 shows the scenario.

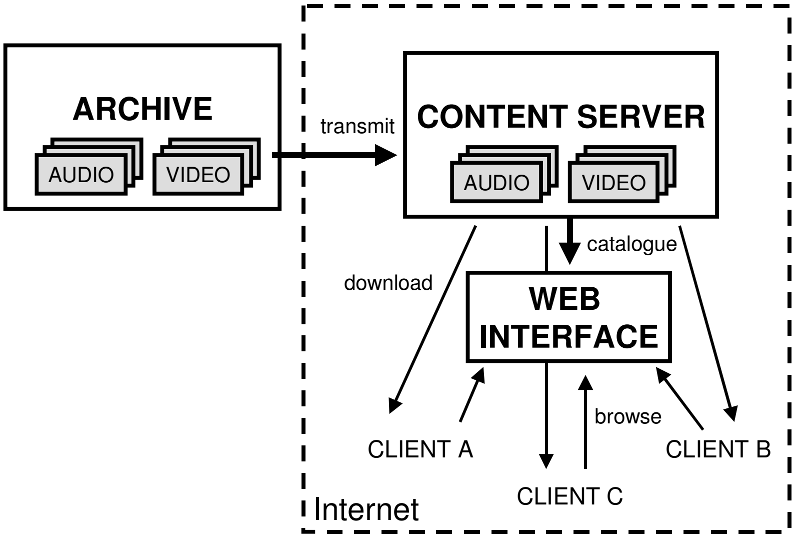


Figure 1: The data of the archive is transmitted to a content server and can be accessed by clients on the internet via a web interface

The DRA has the following requirements regarding the distributed material:

- **Ownership Protection**
  Each transmitted file should be marked with an original ownership label of the DRA.
- **Media and integrity identification**
  Each transmitted file should be marked with a label to identify the content and prove the integrity.
- **Expiration date**
  The material provided by the DRA for media transmission may only be used for a certain time. When the expiration date is reached, payment for using the material has to be renewed. This date has to be embedded into the material so an automatic detection and a notice to the user is possible.

Regarding the security measures identified in chapter 1, the requirements are:

- **Confidentiality** is necessary as third parties should not be able to copy anything a client has requested and paid for.
- **Data authenticatio** has to identify the DRA as the original owner. Data integrity should be ensured as the material of the DRA is used for research and media reports. A change of content could lead to misunderstandings or a change of facts.
- **Entity authentication** is used to identify the customers, legal or illegal copies and to restrict access to preferred or authorized user groups like the DRA archivists.
- **Non-repudiation** is necessary to ensure orders and payments between the client users and the archive.

3. SOLUTIONS FOR OWNER AUTHENTICATION

In the field of owner and customer authentication we can use the already mentioned three classes of authentication methods [16]: (i) possessions (what you have); (ii) knowledge (what you know); and, (iii) biometrics (unique personal traits). Cryptographic and steganographic methods are mainly based on possessions and knowledge of keys, in contrast biometric approaches use unique personal features. In this section we summarize the main cryptographic approaches based on keys and biometric methods.

3.1. Key-based Solutions

Cryptographic authentication of an owner can be realized by means of secret-key cryptosystems and public-key cryptosystems. Here, special aspects with respect to the keys have to be taken into account: Initially, secret keys of secret-key cryptosystems and also private keys of public-key cryptosystems must be stored in such a way, that they can not be stolen or manipulated. Also digital watermarking approaches require keys for embedding and retrieval of digital watermarks, where yet particularly symmetric stego keys are being used [3, 10]. These secret symmetric keys remain in the possession of the creator of the watermark information, i.e. the copyright holder.

Altogether a secure carrier is needed, where only its legal owner is able to activate or to use those keys for security-related computations e.g. the generation of a digital signature, encrypting data or processing authentication protocols. Usually a smart card is used, where its owner authenticates himself in two different ways by possessing the security token and the knowledge of a PIN that is needed to get access to the card.

Using public-key cryptosystems, additionally, the following problems arise:

- Regarding cipher systems: The public key of the recipient is needed to encrypt data. This key must be authentic for each encrypting entity, i.e. the key must have integrity and must be owned by the legal recipient. If its authenticity can not be checked, an attacker is able to generate its own key pair and publish the public key bound to a wrong identity. Claiming the wrong identity, he gets knowledge of information in an unauthorized way (impersonation attack).
- Regarding digital signature schemes: The public key of the signer is needed for the verification of the digital signature. By means of the verification key, the signature concerning to specific data can be verified and therefore, the authenticity of the data can be checked. But it can not be checked whether the verification key belongs to the right signer or not, and furthermore, who generated the signature.

  Thus, the signer of a message can repudiate that he owns the verification key and therefore, that he is the legal signer of the message. Additionally, the verifier can claim that the verification key does not belong to an entity which claims to be the right signer of the message (repudiation attack). Even the verifier must be sure that the public key used for the verification of signed data belongs to the legal producer of the signed document. If this can not be fixed, an attacker might be able to produce his own key pair, fake signatures and claim to be the right signer (impersonation attack).

These examples show that there is a need for an authentic link between the public key and its owner. Such a link can be provided by so called public-key certificates [6,17,18,19]. Public-key certificates used for security measures include all relevant items, which are necessary for a unique identification of an entity. Since 1986, different versions of public-key certificates have been defined specified in ASN.1-notation. During the past, the practice has shown the need for additional granularity of the specification of certificates. Today, the current version v.3 of X.509 certificates allows to use a lot of extensions, where some of them can be used for propriety purposes, e.g. for defining attributes of an entity like roles, rights or authorizations. For issuing certificates a trustworthy authority, a so-called trust center (TC), together with a complex public-key infrastructure is needed. Trust centers authenticate the link of users to their public keys, and can provide further services like non-repudiation, revocation handling, timestamping, auditing and directory service.

3.2. Biometric based Solutions

Biometric based authentication systems make use of statistical analysis of biological characteristics of human beings, which are linked to the documents subject to authentication. Such characteristics can be classified in physical (passive) characteristics such as fingerprints, palm-prints or features of the eye (retina or iris) and behavioral characteristics (active) like handwriting, voice or keystrokes. The aim is to match an actual sample of one ore more characteristics against a reference dataset, in order to verify or identify a particular user. A prerequisite for this matching is the process of capturing reference data and registering this template along with user specific information, which is called enrollment. Whilst for verification, a biometric system only needs to access the pretended user's reference, an identification requires access to the database containing references of all registered users. Further, a biometric verification or identification system can make use of one single characteristics (uni-modal system) or compares several different characteristics and draws an overall conclusion regarding the authenticity.

Once an user is enrolled, there are three possibilities to assign individual reference data to a multimedia document for later authentication: either the reference data can be embedded directly in the document, or a biometric fingerprint is stored along with the payload. The third possibility, which will be discussed more detailed in chapter 5.2, is to store a key (e.g. for embedding a watermark) in a key retrieval system with biometric access control.

4. SOLUTIONS FOR DATA AUTHENTICATION

4.1. Cryptography Solutions

The following two mechanisms assure data origin authenticity:

- message authentication code (MAC), and
- digital signatures.

These mechanisms are detective, and the protected data again remains in plaintext.

A message authentication code (MAC) is a one-way hash function h = H(k,m), which is parameterized by a secret key k. The security of a MAC depends on the length of the generated hash value as well as on the quality of the used key k. Only those entities that know the secret key k may calculate the MAC. The mechanism works as follows (see figure 2):

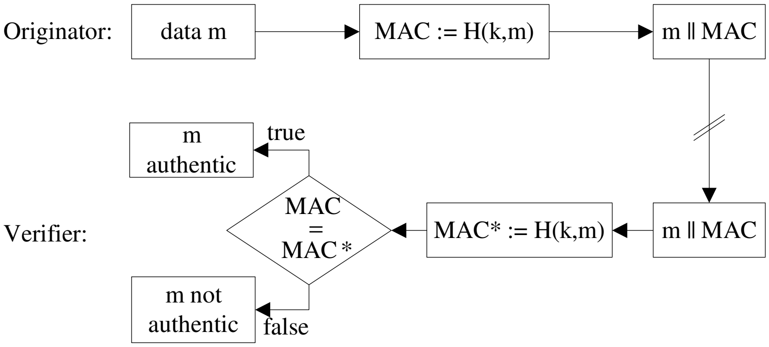


Figure 2: Message Authentication Code (MAC)

The originator who wants to protect the data m calculates a checksum of m using a one-way hash function and the key k, i.e. he computes MAC := H(k,m). Anyone who owns key k can check data m for authenticity. For this the verifier computes a checksum MAC* := H(k,m). If this value corresponds to the original MAC, data m (and also the MAC) are authentic. Otherwise either m or the MAC has been changed in the time period between the generation of the MAC and its verification process.

It is important to note that for this mechanism to work at least two parties, namely the originator and the verifier, need to hold the same key k. Thus, a MAC can not be used to prove anything (e.g. transmission or authenticity) to a third party.

Another mechanism for data authentication are digital signature schemes. Here, the digital signature of an entity A (the signer) to data m shall depend on the content of m and, additionally, on some secret information only known to the signer. Each user shall be able to verify the authenticity of the signature created by A (verification), by using a publicly available information of A. Since only A possesses the secret information, only he is able to create the signature to m by using the signing function S. Therefore, unlike the MAC, the digital signature may be used to prove some fact (origin, authenticity) to a third party.

The functions used for generating a digital signature are called trapdoor one-way functions These functions are one-way functions in the following sense: given a preimage x it is easy to calculate the image f(x), but it is computationally infeasible to find a preimage x for any given f(x). However, if some additional information y (called the trapdoor information) is known, it is easy to compute x.

Public-key cryptosystems can be used to generate and verify digital signatures. The secret key SK of a user represents the secret information, and the public key PK the publicly available information.

For protecting the authenticity of data by digital signatures the following steps are performed (see figure 3). The description given here is limited to a simple scheme of a digital signature.

Signer A wants to transmit data m and its signature to a verifier. For this A computes the hash value h of m by means of a hash function h := H(m). Then A calculates the value s := S(SKA,h) by applying the signing function S to H(m) and a secret value only known to him (his secret key SKA). Finally A transmits m and the corresponding digital signature s to the verifier.

The verifier needs to know the public key PKA of A, the hash function H and the verification function V. First he computes a hash value h* := H(m) of the received data m. Then he transforms the received signature using the verification function and the signer's public key, i.e. he calculates h = V(PKA,s). Finally, he compares the values h and h*. If h = h*, A's signature is correct, meaning that neither the data nor the signature have been altered after their generation. Since A is the only one being in possession of the secret key SKA, only A can compute the correct signature s to m. If h ≠ h*, the signature is considered as false and the data as not authentic. This can be caused for example by the modification of the data m or the signature s in the time between the signing and verifying process, or by a public key not corresponding to the secret key used for the signature generation.

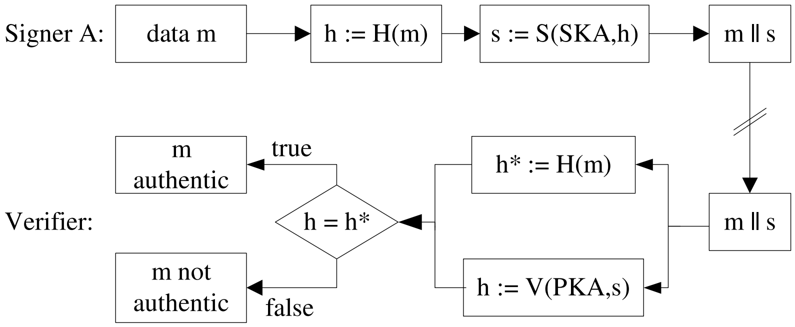


Figure 3: The Principle of a Digital Signature

4.2. Watermarking Approaches

Digital watermarking is a technology for embedding information into cover signals. Robust digital watermarking can be used to claim copyright protection by embedding authors or producers information. Fragile watermarking techniques address the recognition of manipulations.

In general a digital watermark is a perceptually transparent pattern inserted in digital data using an embedding algorithm and a secret key. Basically the principle is to hide a watermark W in a given data C (cover) by modifying some of its characteristics. In the case of visual data it can be the pixels values (luminance, chrominance, color space) or transformed coefficients. In all cases the quality of the watermarked data must be as close as required by the application to the quality of the original.

To secure the watermark the embedding modules E are parameterized by a secret key. The goal of the secret key is to make the watermark secure against removal or replacement. Ideally, the watermark can neither be read nor removed without knowing this key. The watermarking embedding strategy can be seen as:

$C_W = E(C, W, K)$ (4.1)

In some algorithms, the key K is known by anyone and these schemes are called public watermarking [3]. The role of the key is to produce a diversification between different watermark creators. It is worth noting that some applications do not even need a key, since they are not concerned by security issues. At the receiver side R, the image is analyzed by the retrieval module, with the use of a key or not depending on the embedding module. In today’s schemes the used key is an symmetric key, so we call the approaches private schemes in analogy of cryptography. Also asymmetric, like public key schemes are discussed in literature for example in [2], but public key schemes do not seem to be secure in the moment [12]. The retrieval process is performed as following:

$W = R(C_W, K)$ (4.2a) or $W = R(C, C_W, K)$ (4.2b)

We call (4.2a) blind or oblivious watermarking and (4.2b) non blind or non oblivious watermarking when the original data C is not required.
There are two kinds of analyses [3]:

- Presence Watermarking (One-Bit-Watermark): the watermark is a correlation pattern; it carries one bit information, the retrieval consists in correlating the presumed watermark with an estimated watermark extracted from the analyzed image. The output is the level of confidence in the presence of the watermark.
- Information Watermarking (Bit-String-Watermark): the watermark is more than correlation pattern; it carries usually a number of bits as binary message, the retrieval consists in extracting this message (with or without a correlation pattern) and outputting this message (with or without a level of confidence).

Both schemes differ in the amount of information W we can embed and retrieve.

4.3. Problems and solutions for media data

The goal of data authentication is to ensure the integrity of the protected content. This is an important difference to a cryptographic approach where a complete (perfect) identity is demanded. Media data is often a subject to manipulations not changing its content but its binary representation. Lossy compression algorithms, filter operations and format changes are common examples for content-preserving operations. A content-changing manipulation would be the removal of a relevant object. An important problem here is deciding if a change is content-preserving or content-changing. To detect the changes and to decide if a change of content has occurred, we use features describing the content of the media.

For instance, in audio media, this could be the spectrum, the zero crossing rate, the root mean square or similar features. In video data, edge detection or histograms can be used. For a more detailed discussion of the features and references to different approaches, see [7,26]. This features can be used as input to

- cryptographic authentication functions, called content-based MACs or content-based digital signatures, or
- digital watermarking methods.

The advantage of watermarking is, that the integrity information is directly related to the content and presents no additional data like signatures or MACs. Therefore we want to look at digital watermarks for authentication in more detail. In general, for data authentication, five concepts exist:

- **Fragile Watermarking:** A watermark is embedded into the cover signal. It is not robust against manipulations and therefore it is destroyed when these occur. Detecting the watermark is the prove of integrity, e.g. [14, 15, 16,20],
- **Invertible Watermarks:** This is a special kind of the fragile watermark. In addition if the data is authentic, the embedded watermark can be retrieved, inverted and the original document can be reproduced, e.g. [13]
- **Semi-fragile Watermarking:** Similar to fragile watermarking, the watermark is embedded and retrieved as a prove of integrity. But here the watermark is robust against allowed manipulations, e.g. lossy compression. After these manipulations, the watermark is still detectable, e.g. [14, 22]
- **Content-fragile watermarking:** As described above, a watermark robust against most manipulations is used to embed a description of the covers content. This description is fragile against content-changing manipulations. A prove of integrity is achieved by comparing the embedded feature information with the covers actual features, e.g. [7, 8, 11, 25]
- **Hologram watermarking:** The special characteristics of a hologram is used together with watermarking technology to create a very robust watermark. Bitmap information describing media content is embedded into the media and later compared with it to detect content changes [4, 5].

Preferred approaches (usually the last two approaches) enable us to identify the nature and/or the exact position of content manipulations as they provide us with information about the original content. These kind of approaches require a higher watermarking payload and are often of a higher complexity. While the first two approaches only consist of the embedding and retrieval steps, more operations are necessary for content-fragile watermarking and hologram watermarking:

Step 1: Content retrieval: A feature detection algorithm is used to analyze the media file and retrieve content-describing information.

Step 2: Feature Watermark creation: The retrieved features usually can not be embedded directly, so operations like calculation feature checksums (see section 5.1) or building graphical representations for the hologram approaches are necessary.

Step 3: Embedding: As in all watermarking approaches.

Step 4: Retrieval: As in all watermarking approaches.

Step 5: Content retrieval: As in step 1, this time on the marked cover.

Step 6: Feature comparison: The features retrieved in step 4 and 5 are compared to detect changes in the content.

An important requirement for all approaches is that the embedding process of the watermark may not cause a detected change of content. This means, the watermark has either a good transparency and/or the features are robust against the embedding process.

For content-fragile or hologram approaches, we embed the describing features which are much less then the described media. But usually even the reduced data cannot be embedded directly into the media as a watermark. The maximum payload of today’s watermarking algorithms is still too small. To directly embed some content description, we have to use summaries of features or very global features – like the RMS of one second of audio. This leads to security problems: As we only have information about a complete second, parts smaller than a second could be changed or removed without being noticed.

A possible solution is to use feature checksums: We do not embed the robust features but only their checksum. These can be compared to the actual media features checksums to detect content changes. An ideal feature is robust to all allowed changes – the checksum would be exactly the same after the manipulation.

We have further to investigate the characteristics of feature descriptions or checksums regarding their robustness and their security. As they only provide a kind of media hash, specialized attacks could be possible to change the content without changing the features checksums: If a attacker knows the used feature, he could try to copy the original feature characteristics to the changed material.

5. FRAMEWORK

Based on the presented data and owner authentication mechanisms we introduce our framework design for the H2O4M scenario in this section. Furthermore we describe our designed general approach for biometric authentication and an example approach for content-fragile watermarking for digital images.

5.1. General framework for H2O4M

In section 2 we describe the DRA-scenario and identify the requirements confidentiality, data authentication, data integrity, entity authentication and non-repudiation. Now, after describing different security mechanisms, we want to show how they can be used in combination to satisfy the requirements. Figure 4 shows the DRA scenario from section 2, this time with connected security mechanisms and interface points.

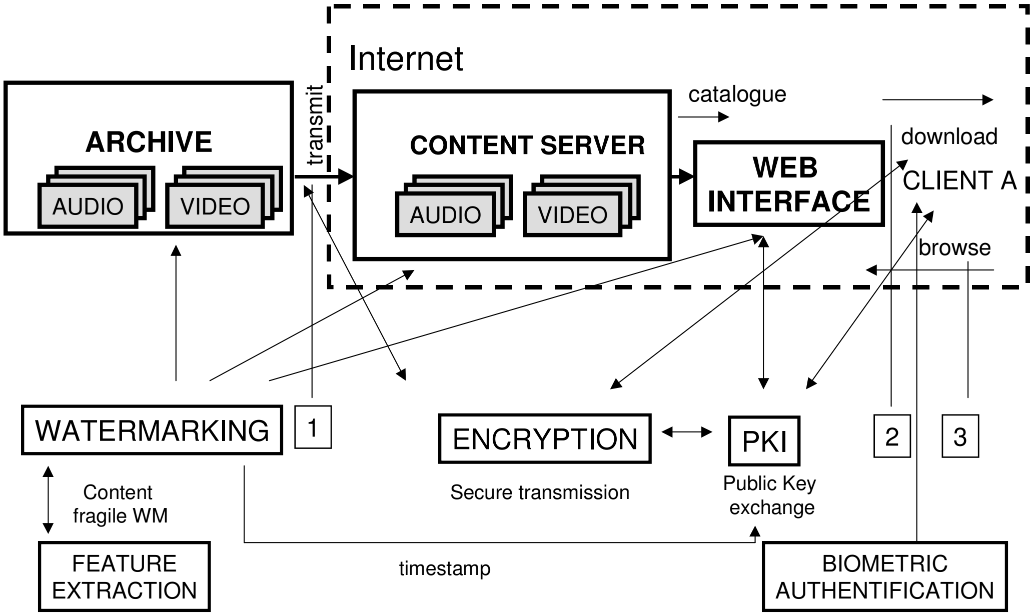


Figure 4: Example framework and security mechanisms

Confidentially is achieved by cryptography: Especially the transmission of the media content from archive to content provider (1) and from web interface to client (2) over the internet has to be protected against piracy. The communication between client and web interface (3), e.g. ID exchange or payment information, should also be secured. In the later case PKI solutions are preferred as they provide a secure framework for key exchange. For media transmission a symmetric / asymmetric session key scheme is applied.

Data authentication has to be applied at the archive to ensure a maximum of security. A robust watermark can be embedded or a MAC can be created to identify the DRA as the original owner by requiring the knowledge of secret keys used for embedding or encryption. To add security against third party claims of ownership, timestamps based on media content information can be applied to the watermarking information. Data integrity protection is necessary at (1) and (2). It can be provided by either hash functions or content-fragile watermarking. Both ensure the integrity of the media data. The later is also robust against content-preserving manipulations and is therefore preferred when one integrity protection mechanism should stay active from archive until client. Additionally, content-fragile watermarking is also present after transmission to the client and later enables third parties to detect changes the client made in the media. If a maximum of data integrity is required, only MACs, certificates or reversible watermarking mechanisms are allowed. In section 5.3 we describe a general concept for data authentication by content-fragile watermarking.

Entity authentication is necessary at (1) and (2): Content-server has to ensure that only material from the archive is uploaded. As this will be an automatic process, keyword protocols based on cryptography will be used. In the case of client identification, alternatives to common key ID methods can be used. Biometric authentication in combination with a secure communication can be used in (2). For authentication of the content server, again cryptography-based mechanisms are necessary. In section 5.2 we describe a general authentication concept based on biometrics.

Non-Repudiation is important in (2) to ensure the client will pay for downloaded material. It can be achieved by protocols using the mechanisms as mentioned above. Timestamps and cryptographic mechanisms combined with biometric authentication can provide a secure record of the client download request and the following successful download.

The specific demand of the DRA to include expiration dates in the data can be satisfied by embedding robust annotation watermarks at the time of the clients' download process.

5.2. Generic approach for biometric owner authentication

Cryptographic and watermarking schemes require key management strategies. Providing an authentic link between a public or symmetric key and an owner is a major problem of key management and can be solved using biometric verification techniques, like introduced in [27, 4]. However, all biometric systems are subject to errors in the authenticity decision step. In order to optimize the decision results, we propose a new decision system, which not only takes the similarity, but also an obvious dissimilarity of two biometric signals into account. The idea is to significantly reduce the False Acceptance Rate, keeping the False Rejection Rate constant, thus allowing the design of secure key management systems. Our approach is to compare similarities and dissimilarities of reference and test data.

The general system approach was introduced in [4, 27] and is based on the approach to use biometric features for user authentication towards a server. Such a server system must be operated by a trusted certifying instance. Initialization of retrieval can either be requested or unsolicited. In the unsolicited case, the actual biometric input is fed to the certifying system, the system will then attempt to identify the subject and respond with the deposited key, if successful. As introduced in [27] the system is based on several handwriting semantic classes like signature or pass phrase. If we use only one biometric feature, users cannot be authenticated if the users are not able to use their hands for example. Therefore the idea is to record and deposit several different active and passive biometric features per user (e.g. active: voice, handwritings; passive: face, fingerprint). This allows the system to have an backup strategy if one biometric feature is not present and to perform a multi level authentication additionally. If the authentication request cannot verify the user positively further authentication requests (AD) will be preformed. We call this approach multi-modal biometric verification.

To optimize the decision results, we propose a decision system based on the heuristic, that some features represent similarity of passive features, where others are indicators for behavior and active similarity. In order to differentiate between the two classes "passive dissimilarity" and "active similarity", we assign two programmable weights to each feature vector F_i, denoting the relevance for either of the classes. Two new programmable weights are introduced: w_{Ai} is the relevance of feature set i towards passive dissimilarity, whereas w_{Fi} weights the relevance towards active similarity. Weights may be in the range of [0..1], where 0 denotes maximum and 1 means minimum relevance.
Based on this classification and the introduced weights we propose the new verification system that evaluates two contrary hypotheses:

- H_A *– Hypotheses biometric feature is authentic*, with Δ_A being the weighted distance measure between the test sample S and the reference R
- H_F *- Hypotheses biometric feature is a forgery*, with Δ_F being the weighted distance measure between the test sample S and the reference R

Applying a distance measurement between each feature vector F_i of the test feature sample and the corresponding reference R_i tests both hypotheses. However in our scheme, each F_i will be assigned two hypotheses weights w_{Ai} and w_{Fi} representing the relevance of feature for either hypotheses. As a result, we compute two similarity measures describing the weighted distance between test feature and reference in both classes. Following the classification scheme, we extend the decision process into two class decisions. For both classes, an independent decision if the biometric feature can be verified or not, will be drawn. For either of the cases, threshold values t_A and t_F are being introduced and each class decision is determined as follows:

$$S\ is \begin{cases} active\ \ verified\ towards\ R, if\ \ \Delta_A(F,R) < t_A \\ active\ \ falsified\ towards\ R, if\ \ \Delta_A(F,R) \geq t_A \\ passive\ dissimilar\ towards\ R, if\ \ \Delta_F(F,R) \geq t_F \\ passive\ similar\ towards\ R, if\ \ \Delta_F(F,R) < t_F \end{cases} \tag{5.1}$$

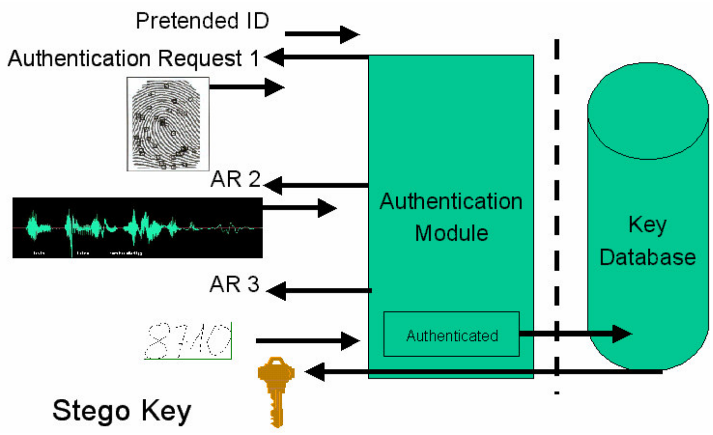


Figure 5: Multi-modal authentication for key retrieval

The overall verification decision is dependent on each class decision. Due to the nature of the global distance functions Δ, the two class decisions are statistically dependent. In order to allow compensation of a poor similarity measure in one class by a strong value in the other, we introduce a trade-off computation, which will be bounded by a trade-off limit value L. In order to apply the trade-off, we introduce advantage values α_A and α_F for both classes. The value of trade-off limits can be assigned on a person or system level. A trade-off limit of 0 means that both class decisions must be positive in order to achieve an overall verification. If a value is chosen, which in sum to the predefined threshold exceeds the value 1, the system will verify each feature that is accepted by either of the class decisions, regardless of the result of the other.

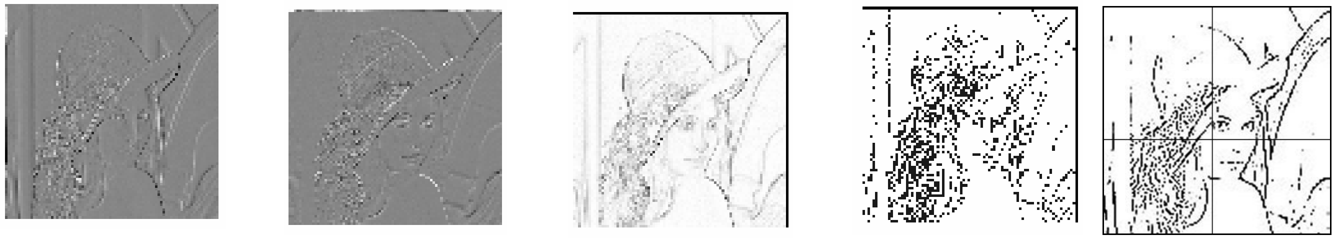
The results of our initial testing based on handwritings of different semantic classes proof that the concept of our new decision module can be applied successful and it can be expected that it allows significant reductions in error rates of verification systems and thus allows design of robust and safe key certifying server systems. However testing of the new scheme is computationally expensive and the number of test subjects was limited in the initial test.

5.3. Content-fragile approaches by Delaunay triangles

Our goal in this section is to introduce a fragile watermarking scheme to allow content-preserving manipulations like scaling and compression to detect content changes. As allowed operations we assume the following modifications: brightness, contrast, scaling, noise, sharpen, JPEG-compression and format conversion. Adding and removal of objects are forbidden manipulations. As introduced in [11,25] one main principle it to derive the content description from the edges, in our case obtained by a wavelet transformation. Thus is not possible to secure all the edges in the picture the other idea is to compute statistical data from the accumulation points further called Center of Gravity. These points are used as input for the Delaunay triangulation. The luminance based watermark pattern are embedded into these triangles. The difference to the method of [1] which also uses the Delaunay triangulation [23] is that they compute the points for the triangulation with schemes from Harris and from Achard-Rouquet. In contrast their goal of the processing is to obtain a robust watermark scheme.

The overall idea of our algorithm is to obtain a content-description and then embed a robust watermark in this significant places. The points representing the edges will be used to compute the accumulation points as gravitation centers which are the basis of the triangulation process used as watermarking position. After the Delaunay step, the algorithm generates a pattern based on a key which will be embedded into the triangles. Therefore if the content is changed the watermark cannot be extracted.

For our algorithm we recognize edges in an image by using the wavelet in the variant proposed by Mallat [23]: the Modulus Maxima procedure. The result matrix contains the Wavelet Modulus Maxima for an image. In order to be able to derive the edges from this matrix, the values need first be standardized. Then the determination of a threshold value T in the range $0.2 \leq T \leq 0.8$ takes place, to avoid considering spurious edges. Figure 6 shows in the pictures (a) and (b) the effects of a wavelet transformation to lena.jpg. Picture (c) shows all modulus maxima of the transform and (d) only the ones above a given threshold. The resulting image (d) represents the abstract content from which our fragile watermarking pattern position will be derived. To achieve this mapping we compute the accumulation points of points visible in (d).



(a) (b) (c) (d)

Figure 6: Horizontal(a) and vertical (b)Wavelet Transform, Wavelet Transform Modulus (c), Wavelet Transform Modulus Maxima above a given Threshold (d) and first center of gravity of lena.jpg (e)

The choice of CG (Center of Gravitation) as a reference point is no coincidence. The gravitation points are equal to the accumulation points mentioned above. Let the wavelet maxima locations be (x_i, y_i) where (x_0, y_0) is the coordinate of the center of gravity of wavelet maxima

$$x_0 = 1/N \sum x_i, \qquad y_0 = 1/N \sum y_i \qquad \text{i = 1…N-1} \qquad (5.2)$$

and N is the total number of wavelet maxima (edges) in the whole image. (x_0, y_0) represents a statistical value of image edges and is now used as content reference point for our watermarking positions. Figure 6 (e) shows the first center of gravity obtained from the described data. We use the [21] as watermark pattern and show now how the CG is used to calculate the watermark positions. The resulting reference points are depending on the edges and they represent statistical values. So the reference points should not change as long as the image are not manipulated by means such as adding or erasing image elements. To embed now the watermarking pattern from [21] we first compute the Delaunay triangulation based on the reference points. It is necessary to use the same triangles in order to embed and retrieve the watermark. Therefore we use the Delaunay triangulation which possesses two important properties. The row continuation of the points provided by the algorithm is not essential in order to always obtain the same triangles as well as the same triangulation. The triangles built by the Delaunay triangulation possess high angles. Consequently, they cover a relatively large area.

The left picture on Figure 6 shows an example for the described triangulation. The idea is how to use the CG as reference point for our watermark position, where we embed the generated watermark patterns of [21] based on a Delaunay triangulation. To recapitulate:

1. The image will be transformed into a gray scale image.
2. The wavelet transformation will be performed on the gray scale image.
3. After the transformation on the transformed image data, the threshold process will be executed. The threshold determines the number and the precision of the edge detection. Thus it is possible to filter or show weak edges.
4. The points now representing the edges will be used to compute the "Center of Gravitation" as a reference point.

From this CG we derive now our watermarking positions:
At the base of this reference point, the image will be divided into four parts which are not required to have identical sizes (the size should be key dependent). The same procedure will be performed on each of the four divisions consequently. The new image parts do also have reference points. After performing this procedure iteratively, we obtain a number of reference points, in function of the iteration steps.

Now the watermark is embedded as described in [21] as a luminance watermark. Only the blocks in any triangle will be marked with the watermark pattern and not all blocks of an image. On the right side of figure 7 we see the difference between the original and the watermarked image. Only the points within the triangulation area have been marked. To avoid that only textured areas are marked, like in figure 7 the centered area, we can add the image corners to the edge list.
The algorithm embeds a robust watermarking pattern on content related marking positions based on wavelet calculated edge characteristics, the CG and Delaunay triangulation. Our first development show compromising results to be robust against content-preserving manipulations and to detect content changes. Problems occur with very slight manipulations in small

regions. Currently we improve the detection of these kind of small changes by improving the calculation of the center of gravities and using RGB color splits to enhance the algorithm.

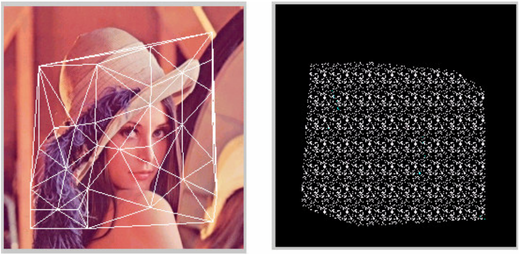


Figure 7: Screenshot showing the triangled and difference image

6. SUMMARY AND FUTURE WORK

Our paper gives an overview of techniques for data and owner authentication possibilities. Out of a variety of techniques we present a framework for our H2O4M scenario and introduce for data authentication a content-fragile image watermarking approach and a generic biometric owner authentication system. Thus security of these mechanisms is mainly based on the authenticity of specific data like keys and attributes – both data must be dedicated to its owner in an authentic manner. A combination of data and entity (owner) authentication are an essential part to secure multimedia applications. In the field of content fragile watermarking we have to observe the possibilities and limits of derived content features in more detail and also design approach for audio and video.

The implementation of the described DRA scenario is planned for the future. Based on this implementation, results regarding the usability of the different discussed security mechanisms will be made available.

ACKNOWLEDGMENTS

The research work about Delaunay triangulation described in this paper was performed jointly with Zülfükar Onay and Carlos Pereira. Astrid Mayerhöfer supported the design and evaluation of the biometric approach. We would like to thank them for many stimulating discussions and support.

REFERENCES

1. P. Bas, J-M. Chassery and B. Macq, “Robust Watermarking Based on the Warping of Pre-Defined Triangular Patterns”, in Proceedings of SPIE: Security and Watermarking of Multimedia contents II, 24-26 January 2000, San Jose, California, Vol. 3971, pp. 99-109, 2000.
2. S. Craver, S. Katzenbeisser: Watermarking: The Ticket Concept, in Steinmetz, Ralf; Dittmann, Jana; Steinebach, Martin (Eds.): Communications and Multimedia Security Issues of the New Century, Volume 192, Kluver , ISBN 0-7923-7365-0, pp. 53-65, April 2001
3. J. F. Delaigle: Protection of Intellectual Property of Images by Perceprtual Watermarking, PhD-Thesis at LABORATOIRE DE TELECOMMUNICATIONS ET TELEDETECTION, UCL, Belgium, September 2000
4. Dittmann, J.; Steinebach, M.; Croce Ferri, L.; Mayerhöfer, A..; Vielhauer, C.: Advanced multimedia security solutions for data and owner authentication; Applications of Digital Image Processing XXIV, Proceedings of SPIE Vol. #4472, (2001), 29 July - 3 August 2001, San Diego, California, USA
5. Dittmann, J.; Croce Ferri, L.; Vielhauer, C.: Hologram Watermarks for Document Authentications; IEEE International Conference on Information Technology: Coding and Computing; IEEE Computer Society; Las Vegas, NV, USA, April 2-4, 2001; p.60-64
6. Dittmann, Jana; Nahrstedt, Klara; Wohlmacher, Petra: Approaches to Multimedia and Security, in Proceedings of IEEE International Conference on Multimedia and Expo, 30 July - 2 August 2000, New York, USA, ISBN 0 - 7803 - 6536 - 4, pp. 1275 – 1278, 2000
7. Dittmann, Jana: Content-fragile Watermarking for Image Authentication, to appear in Proceedings of SPIE: Security and Watermarking of Multimedia Contents III, 21 - 26 January, San Jose, California, USA, Vol. 4314, 2001
8. J. Dittmann, M. Steinebach, I. Rimac, S. Fischer,R. Steinmetz: Combined video and audio watermarking: Embedding content information in multimedia data, in , In Proc. of the SPIE Conference on Electronic Imaging '99, Security and Watermarking of Multimedia Contents II, 24-26 January 2000, San Jose USA, Proceedings of SPIE Vol. 3971, pp. 176-185, 2000

9. J. Dittmann, A. Mukherjee, M. Steinebach, “Media-independent Watermarking Classification and the need for combining digital video and audio watermarking for media authentication”, Proceedings of the International Conference on Information Technology: Coding and Computing, 27 - 29 March, Las Vegas, Nevada, USA, pp. 62 - 67, IEEE Computer Society, ISBN 0 - 7695 - 0540 - 6, 2000
10. Dittmann (2000). Digitale Wasserzeichen. Springer Verlag, ISBN 3 –540 –66661 – 3
11. J. Dittmann, A. Steinmetz, R. Steinmetz: Content-based Digital Signature for Motion Pictures Authentication and Content-Fragile Watermarking, In Proc. of IEEE Multimedia Systems, Multimedia Computing and Systems, June 7-11, 1999, Florence, Italy, Volume1, pp. 574-579, 1999
12. J.J. Eggers, J.K. Su, B. Girod: Asymmetric Watermarking Schemes, in Sicherheit in Netzen und Medienströmen, Tagungsband des GI-Workshops "Sicherheit in Mediendaten", Berlin, 19. September 2000, Springer Verlag, ISBN 3-540-67926-X, pp. 107 – 123, 2000
13. J. Fridrich, M. Goljan, R. Du, “Invertible authentication”, to appear in Proceedings of SPIE: Security and Watermarking of Multimedia Contents III, 21 - 26 January, San Jose, California, USA, Vol. 4314, 2001.
14. J. Fridrich: Methods for Tamper Detection of Digital Images, in J. Dittmann, K. Nahrstedt, P. Wohlmacher (Eds.), Multimedia and Security, Workshop at ACM Multimedia’99, Orlando, Florida, USA, Oct. 30 – Nov 5 1999, pp. 29-34, 1999
15. J. Fridrich: Image Watermarking for Tamper Detection, Proc. ICIP ’98, Chicago, Oct 1998.
16. J. Fridrich: Methods for Detecting Changes in Digital images, ISPACS99, Melbourne, November 4th–6th, 1998.
17. ISO/IEC 9594-8 | ITU-T Recommendation X.509: Information technology – Open Systems Interconnection – The Directory. Part 8: Authentication Framework, 1993.
18. ISO/IEC 9796: 1991 Information technology – Security techniques – Digital signature scheme giving message recovery.
19. ISO/IEC 9798: Information technology – Security techniques – Entity authentication. Part 1: General. Part 2: Mechanisms using encipherment algorithms. Part 3: Mechanisms using a public-key algorithm.
20. D. Kundur and D. Hatzinakos: Towards a Telltale Watermarking Technique for Tamper Proofing, Proc. ICIP, Chicago, Illinois, Oct 4–7, 1998, vol 2.
21. G.C. Langelaar, J.C.A. van der Lubbe, R.L. Langendijk, “Robust Labeling Methods for Copy Protection of Images”, Proceedings of SPIE Electronic Imaging ´97, Storage and Retrieval for Image and Video Databases V, February 1997, San Jose (CA), USA
22. E. Lin, E. Delp: A review of fragile image watermarks, in J. Dittmann, K. Nahrstedt, P. Wohlmacher (Eds.), Multimedia and Security, Workshop at ACM Multimedia’99, Orlando, Florida, USA, Oct. 30 – Nov 5 1999, pp. 35-40, 1999
23. Mallat, Stephane (1998). A Wavelet Tour of Signal Processing. A Short Presentation by F. Chaplais. in: Academic Press, 1998. http://cas.ensmp.fr/%7Echaplais/Wavetour_presentation/Wavetour_presentation_US.html
24. B. Miller. Vital signs of identity. IEEE Spectrum, 31(2):22–30, February 1994
25. M. P. Queluz: Content-based integrity protection of digital images, in Security and Watermarking of Multimedia Contents, P. W. Wong, E. J. Delp, Eds., vol. 3657, San Jose, California, U.S.A., 25–27 Jan., The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE. ISBN 0-8194-3128-1, ISSN 0277-786X, pp. , 1999
26. M. Schneider and S.-F. Chang: A Content-Based Approach to Image Signature Generation and Authentication, Proc. ICIP ’96 vol. III, pp. 227–230, 1996.
27. Claus Vielhauer, Ralf Steinmetz: “Approaches to biometric watermarks for owner authentification”, to appear in Proceedings of SPIE: Security and Watermarking of Multimedia Contents III, 21 - 26 January, San Jose, California, USA, Vol. 4314, 2001
28. Zhang, David: Automated Biometrics – Technologies and Systems, Kluwer Academic Publishers, USA, ISBN 0-7923-7856-3, 2000