

MEDUSA

DELIVERABLE

D4.1.1 – State of the Art on secure, dependable data transfer



Medical Distributed Utilization of Services & Applications

Project number: ITEA 10004
Document version no.: WP4
Edited by: Paul-Emmanuel Brun

ITEA Roadmap domains:

Major: Content & Knowledge

ITEA Roadmap categories:

Major: Interaction

Minor: Network & computing

This document will be treated as strictly confidential. It will only be public to those who have signed the ITEA Declaration of Non-Disclosure.

HISTORY

Document version #	Date	Remarks
V1.0		Final Version (Approved by PCC)

TABLE OF CONTENTS

1	INTRODUCTION	6
2	EXECUTIVE SUMMARY	7
3	ACRONYM	8
4	REFERENCES	9
5	MEDUSA SECURITY ARCHITECTURE	11
5.1	THE MEDUSA SYSTEM	11
5.1.1	<i>Use cases of the Medusa system</i>	11
5.1.2	<i>Overview of the Medusa system</i>	12
5.2	INFORMATION SECURITY OF THE MEDUSA SYSTEM	13
5.2.1	<i>Introduction</i>	13
5.2.2	<i>Information security strategy</i>	14
6	IDENTITY & ACCESS MANAGEMENT	16
6.1	ACCESS CONTROL MODELS	16
6.1.1	<i>DAC model</i>	16
6.1.2	<i>MAC model</i>	16
6.1.3	<i>RBAC model</i>	17
6.1.4	<i>OrBAC model</i>	18
6.1.5	<i>Example of access control models</i>	19
6.2	ACCESS CONTROL PROTOCOLS, STANDARDS & LANGUAGES	20
6.2.1	<i>IAM standards</i>	20
6.2.2	<i>IAM languages</i>	22
6.3	USER PROVISIONING	24
6.3.1	<i>SPML</i>	24
6.3.2	<i>SCIM</i>	25
7	TRANSMISSION SERVICES	26
7.1	SECURE TRANSMISSION SERVICES	26
7.1.1	<i>Secure sockets layer and Transport layer security</i>	26
7.1.2	<i>IPSEC protocol description</i>	26
7.1.3	<i>Virtual Private Networks (VPNs)</i>	31
7.2	DEPENDABLE TRANSMISSION SERVICES	33
7.2.1	<i>Infiniband</i>	33
7.2.2	<i>Protocol optimization</i>	35
8	FINGERPRINTING AND WATERMARKING	38
8.1	WATERMARKING IN A NUTSHELL	38
8.1.1	<i>Definition</i>	38
8.1.2	<i>Watermark criteria</i>	38
8.1.3	<i>Theoretical model</i>	40
8.1.4	<i>Watermarking application</i>	41
8.1.5	<i>Watermarking classification</i>	42
8.2	WATERMARKING FOR MEDICAL IMAGING	43
8.2.1	<i>Usefulness of watermarking in medical imaging</i>	43
8.2.2	<i>Medical imaging watermarking requirements</i>	45
8.2.3	<i>Watermarking method for medical imaging</i>	45
8.2.4	<i>State of the art of medical imaging watermarking</i>	46
8.3	IMAGE FINGERPRINTING IN MEDICAL APPLICATIONS.....	48
8.3.1	<i>Introduction</i>	48
8.3.2	<i>State of the art</i>	53
8.3.3	<i>Medical content based image retrieval</i>	60

8.3.4	Conclusions	62
9	PRESENT EQUIPMENT AND STANDARD REGULATIONS.....	64
9.1	INTRODUCTION.....	64
9.2	APPLICABLE STANDARDS AND POLICIES FOR MEDUSA.....	64
9.2.1	Context of applicability of standards / policies.....	64
9.2.2	Selection criteria for applicable standards and policies.....	65
10	TRUSTED EXECUTION ON CLOUD NODES.....	70
10.1	REFERENCE MODEL.....	70
10.1.1	Cloud Service Model Perspectives.....	70
10.1.2	Implications of Cloud Deployment Models.....	70
10.1.3	Shared Security Responsibilities	70
10.1.4	Medusa reference security architecture.....	71
10.2	SECURE CLOUD SOLUTIONS	71
10.3	SECURITY IN COMPATIBLEONE ACCORDS PLATFORM.....	72
	APPENDIX 1: FINGERPRINTING & WATERMARKING REFERENCES	74

LIST OF TABLES

Table 1: example of DAC model.....	16
Table 2: access control model overview.....	20
Table 3: RDT formats summary.....	37
Table 4: applications and purposes.....	41
Table 5: applications and purposes.....	45
Table 6: synopsis of the state of the art of medical imaging watermarking.....	47
Table 7: A digital mammogram with inserted artificial calcifications: (a) original mammogram; (b) with artifacts; (c) magnification of some artifacts; (d) subtracted between (a) and (b). The artifacts are highlighted with overexposure during display [CAO 03].....	49
Table 8: Types of image modifications: they can be induced in the content with computer software or by means of image printing, scanning, copying.....	54
Table 9: types of image fingerprints.....	59
Table 10: types of similarity measures for image fingerprinting.....	60
Table 11: types of image features for CBIR use cases.....	62
Table 12: types of similarity measures for CBIR use cases.....	62

LIST OF FIGURES

Figure 1: use case 1: treatment by a single specialist.....	11
Figure 2: use case 2: diagnose by a multiple specialist.....	12
Figure 3: use case 2: transfer to another hospital.....	12
Figure 4: system overview.....	13
Figure 5: example of DAC implementation.....	17
Figure 6: RBAC object model.....	18
Figure 7: OrBAC object model.....	19
Figure 8: example of SOAP envelope.....	21
Figure 9: packet with AH.....	29
Figure 10: packet with ESP.....	29
Figure 11: IPSEC packet with AH.....	30
Figure 12: IPSEC packet with AH and ESP.....	30
Figure 13: using Infiniband.....	34
Figure 14: Common Infiniband network architecture.....	34
Figure 15: watermarking classification diagram.....	42
Figure 16: Medical images security properties.....	44
Figure 17: human fingerprinting and medical image fingerprinting.....	50
Figure 18: Image identification and retrieval.....	51
Figure 19: interactive advertising.....	52
Figure 20: image filtering in UGC platforms.....	53
Figure 21: Affine transforms induced by camcording.....	56
Figure 22: Images rotated with 2°, 3°, 5° and 10° in (a) column and images rotated and cropped in (b) column.....	57
Figure 23: vertical flipping.....	57
Figure 24: television specific modifications.....	57

1 Introduction

This document presents the state of the art on secure, dependable data transfer regarding the MEDUSA environment.

To describe the state of the art on secure and dependable data transfer, we mainly focus on 4 technicals points: how to manage access control to the data with IAM capabilities, how to control data with fingerprinting and watermarking, how to secure data transmission over the network with security and bandwidth optimization solutions, which security standards & policy should apply for healthcare products & services, and finally, an overview of existing solution to secure Cloud architecture.

To cover all this scope, the document is divided into 6 main sections:

- Section 5 will present briefly Medusa use cases, architecture and requirements regarding security needs.
- Section 6 will present a state of the art on Identity and Access Management with the description of the main access controls models, and then, a quick overview of standards and protocols with IAM capabilities, used to secure access to the data in the Medusa environment.
- Section 7 will present some secure transmission techniques, and then, some dependable transmission techniques.
- Section 8 will focus on a presentation of fingerprinting and watermarking to control data.
- Section 9 will present some existing standards and policy for healthcare products, services or service-related products in terms of security.
- Finally, section 10 will present the main security principles regarding the Medusa Cloud reference architecture

2 Executive summary

Secure, dependable data transfer is a very huge problematic that cover many security requirements, such as data security, transmission security, and privacy.

This document aims at describe the state of the art on secure, dependable data transfer, focusing on access control model, protocols and standards, secure and dependable transmission, data tracking, main standards applicable in Healthcare, and cloud security architecture.

3 Acronym

Acronym / Abbreviation	Definition / Meaning
IAM	Identity and access Management
IPSEC	Internet Protocol Security
VPN	Virtual Private Network
IKE	Internet Key Exchange
SA	Security Association
DAC	Discretionary Access Control
MAC	Mandatory Access Control
MLS	Multi-Level Security
RBAC	Role-Based Access Control
OrBAC	Organization Based Access Control
HCA	Host Channel Adaptater
SAML	Security Assertion Markup Language
SPML	Service Provisioning Markup Language
SCIM	System for Cross-domain Identity
X.509	Public Key infrastructure certificate and CRL profile
TLS	Transport Layer Security
XACML	eXtensible Access Control Markup Language
SOAP	Simple Object Access Protocol
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DRM	Digital Right Management
IPR	Intellectual Property Rights
CBIR	Content Based Image Retrieval
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
HSM	Hardware Security Module

4 References

NIST 2013, *Role Based Access Control (RBAC) and Role Based Security*, Available from:

<http://csrc.nist.gov/groups/SNS/rbac/>

HL7 2010, *Role Based Access Control (RBAC) Healthcare Permission Catalog*, release 2, Available from:

http://gforge.hl7.org/gf/download/docmanfileversion/5578/7158/2009Sept_Ballot_HL7_RBAC_HC_Permission_Catalog_v4.12_POST_reconciliation_JAN_2010.docx

IEEE 4th International Workshop on Policies for Distributed Systems and Networks, 2003, *Organization Based Access Control (OrBAC)* Available from:

<http://www.rennes.enst-bretagne.fr/%7Efcuppens/articles/Or-BAC.pdf>

Data and Knowledge Engineering 2012, *Formal enforcement and management of obligation policies*, Y. Elrakaiby, F. Cuppens, N. Cuppens-Bouahia, Available from:

<http://www.rennes.enst-bretagne.fr/%7Efcuppens/articles/dke12.pdf>

OASIS, 2010. *eXtensible Access Control Markup Language (XACML) Version 3.0* Available from:

<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs-01-en.pdf>

IOS Press, 2010, *SecPAL: Design and Semantics of a Decentralized Authorization Language*, Moritz Y. Becker, Cedric Fournet, and Andrew D. Gordon, available from:

<http://research.microsoft.com/pubs/80148/jcs%20final.pdf>

Microsoft, 2007, *Security Policy Assertion Language (SecPAL) Specification*, Available from:

http://research.microsoft.com/en-us/projects/secpal/secpal_security_policy_assertion_language_specification.pdf

NIST SP 800-66-Rev1: *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Oct 2008 Available from:

<http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>

IHE, *IT Infrastructure Technical Framework Volume 1 (ITI TF-1) Integration Profiles* Revision 4.0 - Final Text August 22, 2007 Available from:

http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_4_0_Vol1_FT.pdf

EU 95/46/EC, *European Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Available from:

http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

FDA, 2005, *Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-shelf (OTS) Software*, Available from:

http://www.21cfrpart11.com/files/library/reg_guid_docs/networkeddeviceswithotssotfware.pdf

5 Medusa Security architecture

This chapter describes the Medusa security architecture and use cases, to have a better understanding of the context used for this state of the art. We focus in this chapter on:

- The main Medusa use cases
- An overview of the Medusa system
- A quick introduction to the main Medusa security requirements and their limits.

5.1 The Medusa system

5.1.1 Use cases of the Medusa system

The functionality provided by the Medusa Processing Service is described by the following basic use cases.

Use case 1:

Treating specialist is the only specialist involved. The specialist requires the images taken by medical equipment to be processed by the Medusa Processing Service, so he/she can establish a diagnose.

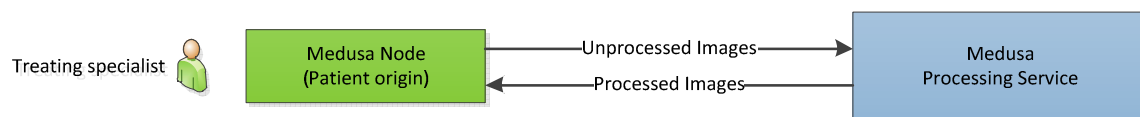


Figure 1: use case 1: treatment by a single specialist

Use case 2:

Treating specialist is collaborating with other specialists to establish a diagnose. In this case the Medusa Processing Service is distributing the processed images to all the specialists involved. The specialists can establish a diagnose. The individual diagnoses made by the specialist are also shared between all the specialists. In this way the specialists can collaborate to establish the correct diagnose.

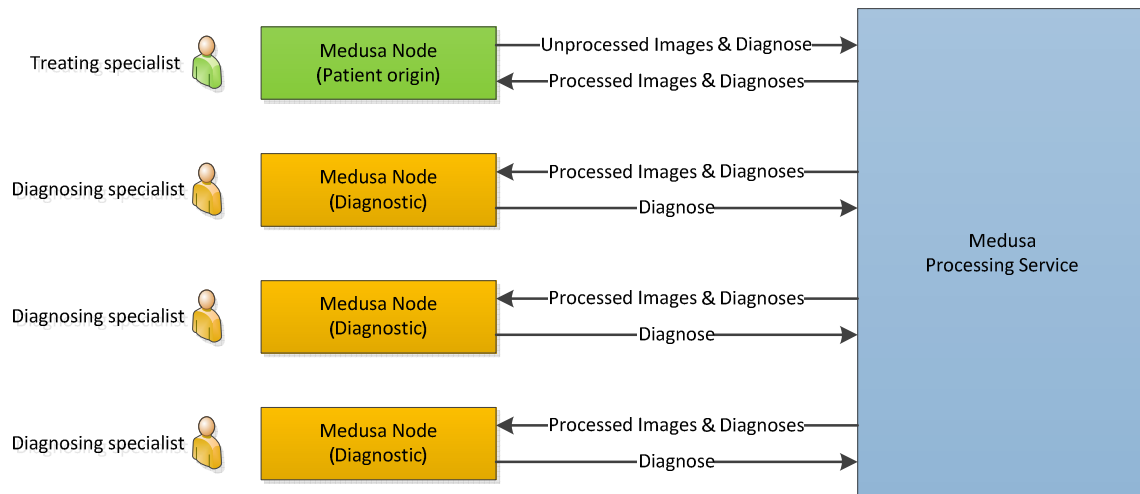


Figure 2: use case 2: diagnose by a multiple specialist

Use case 3:

Patient is transferred to another hospital. The processed images and the diagnoses made by the various specialists are transferred from the Patient origin to the Patient destination by the Medusa Processing Service.

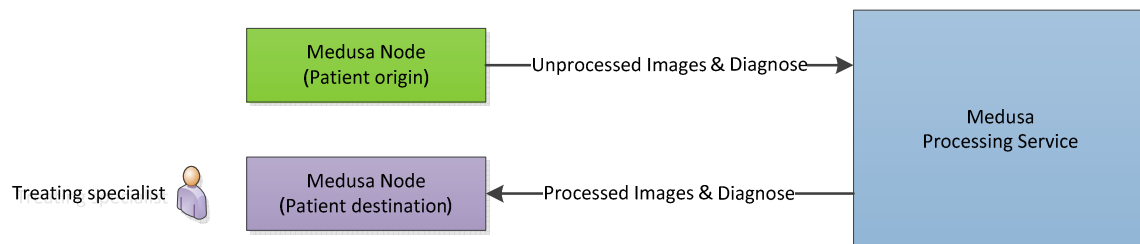


Figure 3: use case 2: transfer to another hospital

5.1.2 Overview of the Medusa system

The system that needs to be “protected” is explained in Figure 4: system overview.

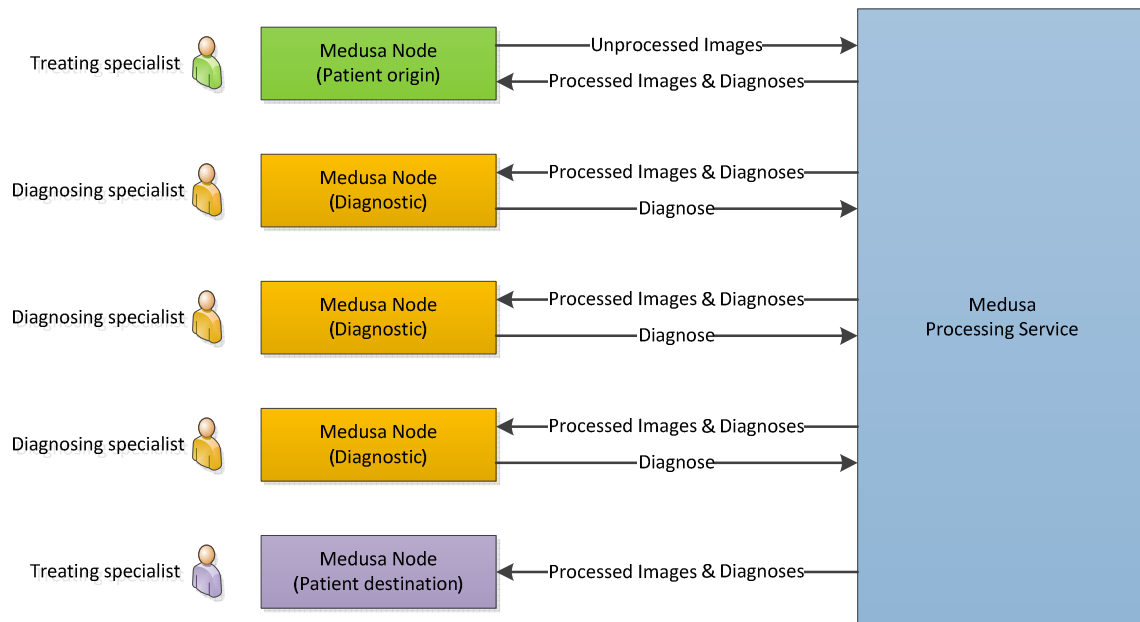


Figure 4: system overview

The goal of Medusa is to let medical specialists share images and diagnostics of these images during the treatment of a patient. The specialists communicate to each other using Medusa nodes. These nodes are connected to the Medusa Processing Service.

During the treatment of a patient a specialist can have 3 different roles:

- treating specialist at the patient origin (this is where the patient is);
- diagnosing specialist;
- treating specialist at the patient destination (where the patient is to be transferred).

The treating specialists at the Origin or Destination may also diagnose the images. Therefore a specialist may have more than one role.

The Medusa Processing Service is able to:

- receive images from the patient origin Medusa node;
- enhance these images for diagnostic purposes;
- send the enhanced images to various Medusa nodes (Patient origin, Diagnostic and Patient destination);
- receive the diagnoses made from various Diagnostic Medusa nodes;
- send the diagnoses made to various Medusa nodes (Patient origin, Diagnostic and Patient destination);

5.2 Information security of the Medusa system

5.2.1 Introduction

The information assets that need to be protected are:

- images (processed and unprocessed) of patient
- diagnoses of patient

These information assets must be protect on the following aspects.

Confidentiality

These information assets are medical records that are private for the patient.

To establish a correct diagnose it is important that the processed images and the diagnoses are shared between a group of specialists that collaborate. This is also the case if the patient is transferred to another hospital. Disclosing these information assets to unauthorized persons must be prevented.

Integrity

The integrity of the information assets is also important. A false diagnose due to incorrect data may have legal ramifications. Therefore it is important that the integrity of the data shared is protected.

Availability

Data needs to be available for authorized persons at the place and moment it is needed.

5.2.2 Information security strategy

Protecting the information assets could be done by adopting the following strategy.

1. Every specialist (or specialist group) communicates with the system via Medusa Nodes. A specialist needs to login to its Medusa Node to gain access to the data sent to that node. Login could for example be done using a username/ password and a token (two factor authentication).
2. There is no fine grained access control implemented on the data in the Medusa Processing Service. When a specialist is logged in it can access all data within the Medusa Processing Service. The reason for this is that this fine grained access control is very cumbersome to maintain and increases the risk of the data not being available to the right specialist on a critical moment.
3. As a corrective countermeasure the Medusa Processing Service maintains a secure audit trail containing which specialist accessed or delivered which data and when. This secure audit trail can be used during a security audit to verify that specialists do not access data when there is no need for it.
4. The Medusa Processing Service is not intended to collect all the data that passes through it and store it forever. When there is no need to keep the data in the Medusa Processing Service it will be erased.
5. Before the data is erased on the Medusa Processing Service the data is synchronized to the Medusa Node of the treating specialist. The secure audit trail of the data concerned could also be sent to the treating specialist. In this way the specialist can see which colleagues have accessed or delivered the data.

6. All the data is signed by a digital signature from the Medusa Node from which it originates. This digital signature is validated when this data is received by another Medusa Node. These digital signatures provide a mechanism to protect the integrity of the data that travels through the system. Secure audit trails are signed by the Medusa Processing Service itself.
7. All communication between Medusa Nodes and Medusa Processing Service is protected against eavesdropping using for example a secure tunnel like SSL.

6 Identity & Access management

In this section, we will present different models, protocols and languages used for Identity and Access Management in IT infrastructure and cloud environment.

Identity and Access Management objective is to manage the user lifecycle and all its impact on the IT system (account creation, account modification, rights modification ...). An IAM solution is global, and should be manage with:

- Functional point of view (ex: Human resources).
- Technical point of view (ex: database administrator).

First, we will present the main identity and access management models, and then, we will study the main languages and protocols used in cloud infrastructure.

6.1 Access Control models

6.1.1 DAC model

DAC (Discretionary Access Control) model has been defined by Trusted Computer System Evaluation Criteria. It allows to restrict access to objects regarding user identity, or groups. Discretionary controls means that a subject with specific authorisation is able to pass that permission to any other user or group.

DAC model is mainly used in IT access control systems, such as the Unix file mode which has write (w), read (r) and execute (x) rights for each user. If a user creates a resource, he will own this resource and have r, w, x rights on it.

	John's files	Henry's files
John	rwX	-
Henry	r	rwX
Marc	rw	r

Table 1: example of DAC model

In this example, discretionary controls allow John to pass r, w, x rights on its own file to the other users.

6.1.2 MAC model

MAC (Mandatory Access Control) model allows to restrict access to objects regarding user identity. However, in the opposite of the DAC model, users are not allowed to grant access to files that they own, or to change the security policy. This model, allow administrators to define a security policy that is guaranteed to be enforced for all users.

An IT system which implements a MAC model is named (MLS) Multi-Level Security.

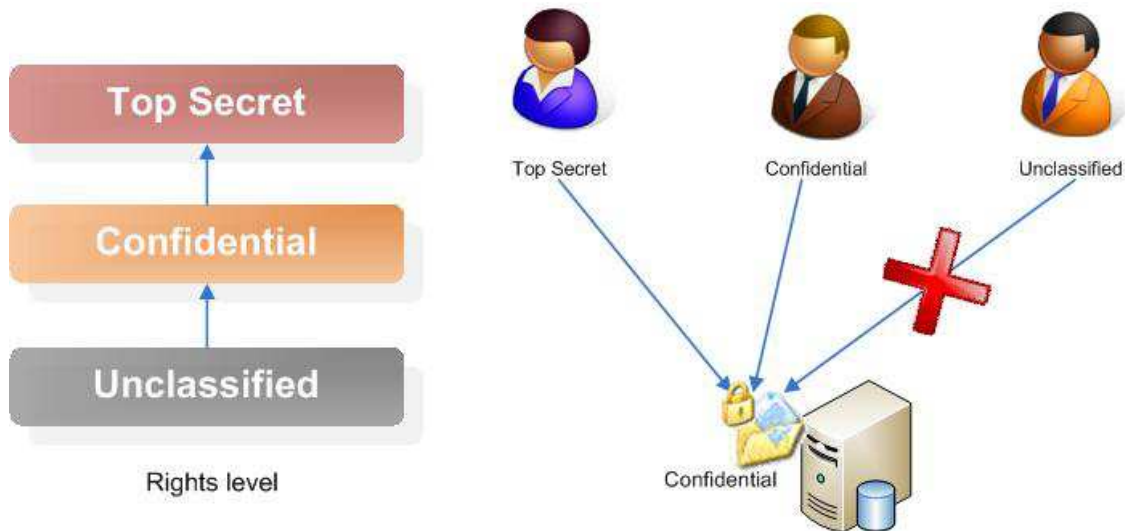


Figure 5: example of DAC implementation

6.1.3 RBAC model

RBAC (Role-Based Access Control) model is mainly used in large organizations. It can implement Mandatory Access Control, such as Discretionary access control.

RBAC model is based on job functions to give access to resources. The permissions to perform operations linked with a job function are assigned to specific roles. Then, management of individual rights is limited to role assignment to a user. In huge systems, this simplifies common operations such as user arrival, user modification, ...

The concepts used by RBAC model are:

- Subject: it is the user in the IT system
- Role: job function in an organization, or in a limited perimeter
- Object: object to protect
- Operation: an action to perform on an object
- Permission: authorisation to perform an operation on an object
- Session: timeslot of the action, each session is associated to a user during a limited time

RBAC object relations are:

- A subject can have multiple roles
- A role can be assigned to multiple subjects
- A role can have many permissions
- A permission can be assigned to many roles
- A permission is a set of operations on an object
- A session could be restricted to one role
- A session is limited to one user

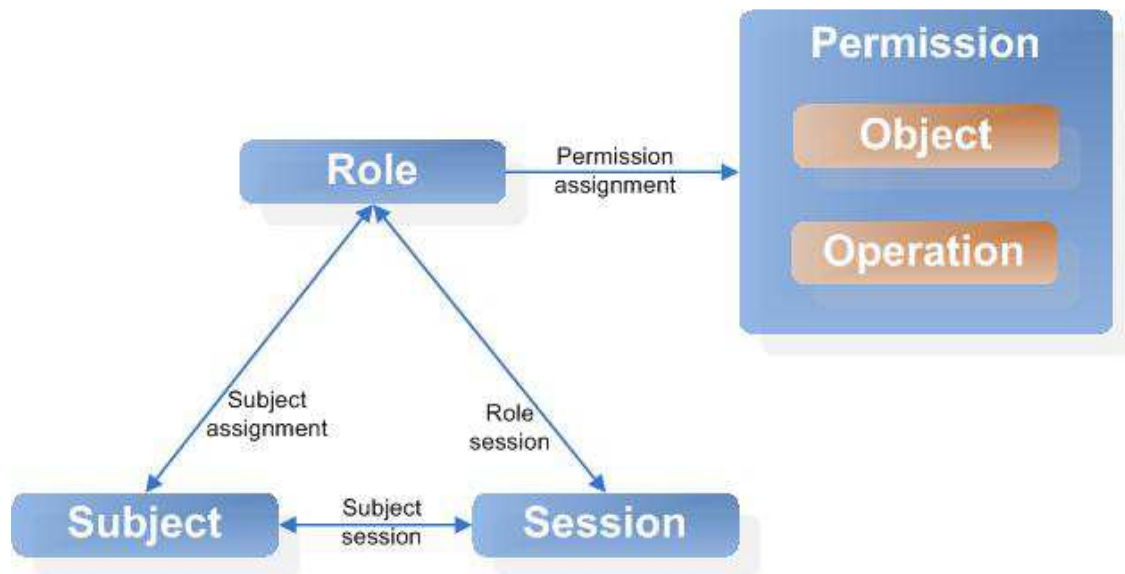


Figure 6: RBAC object model

6.1.4 OrBAC model

OrBAC (Organization Based Access Control) was first introduced in 2003. In this model, a security policy is linked with an organization, and rest on 3 entities:

- Subject
- Action
- Object.

OrBAC model is able to define security policy based on permissions, but also on prohibitions and obligations. OrBAC also offers the possibility to define a security policy independently of the implementation by introducing an “abstract level” where:

- Subject are abstracted into roles, which is a set of subjects
- Action are abstracted into activity, which is a set of actions
- Objects are abstracted into view, which is a set of objects

Each security policy defined applies to a specific organization, which make it possible to handle multiple security policies associated to different organizations simultaneously.

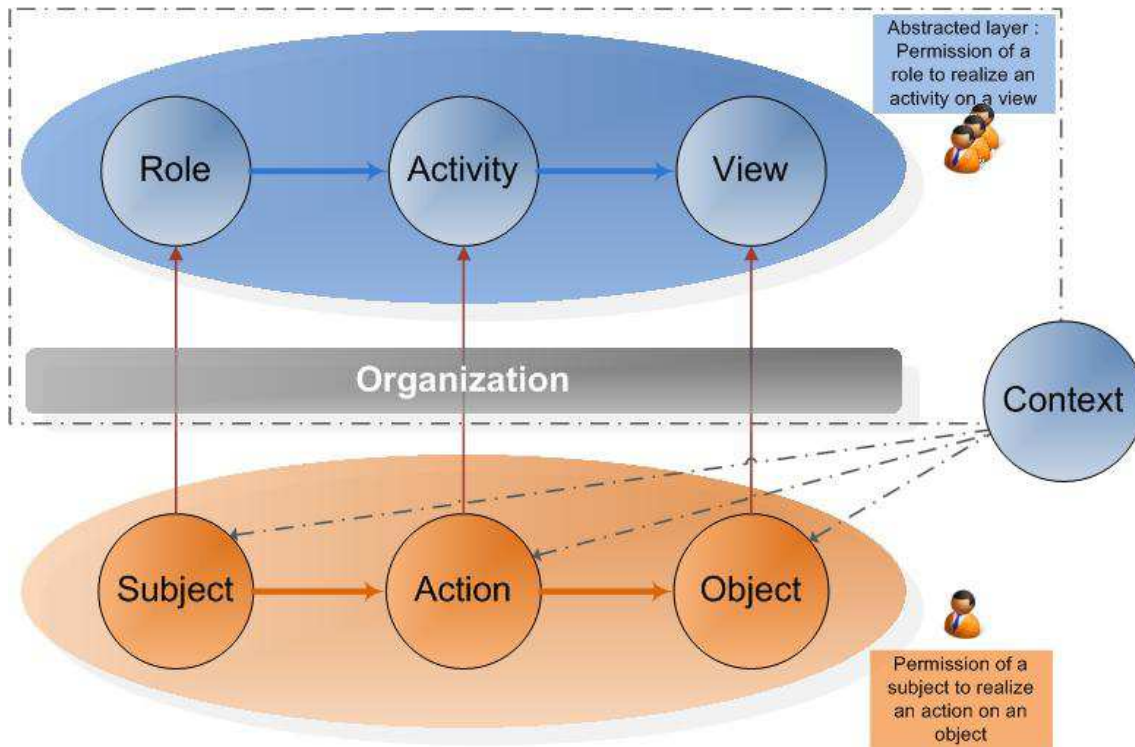


Figure 7: OrBAC object model

6.1.5 Example of access control models

In order to provide some explanation about those access control models implementation, we defined a general situation to compare the differences between those DAC, MAC, RBAC and OrBAC models.

The situation is the regulation of the access control to a patient file for a trauma leader from the hospital A, and a facial surgeon from the hospital B.

Access control model	Example in healthcare environment
DAC	The trauma leader of the hospital A is able to grant the facial surgeon from the hospital B access to the patient file he creates.
MAC	The trauma leader is not allowed to give any access on the patient file he creates. This access is predefined by the security policy.
RBAC	The trauma leader from hospital A will have the same access rights than the trauma leader from hospital B.

OrBAC	The trauma leader from hospital A will have different access rights than the trauma leader from hospital B.
-------	---

Table 2: access control model overview

6.2 Access Control protocols, standards & languages

This section will present Identity and Access Management protocols and standards relevant for cloud infrastructure. Those solutions provide federated Single Sign On, signature capabilities, and also right management, to reinforce security and usability of cloud infrastructure.

6.2.1 IAM standards

6.2.1.1 SOAP

The Simple Object Access Protocol (later referred to only as SOAP) is an XML-based protocol specification for exchanging structured information in Web Services. It was originally introduced in 1998 and the current version, V1.2, was published as a recommendation of the XML Protocol Working Group of the World Wide Web Consortium (W3C) in 2003.

SOAP uses the Extensible Markup Language (XML) for its message format, and usually relies on other application layer protocols, most notably Remote Procedure Call (RPC) and Hypertext Transfer Protocol (HTTP), for message negotiation and transmission. SOAP can form the foundation layer of a Web services protocol stack, providing a basic messaging framework upon which web services can be built.

SOAP consists of three parts:

- an envelope, which defines what is in the message and how to process it
- a set of encoding rules for expressing instances of application-defined data types
- a convention for representing procedure calls and responses

The SOAP specification defines the messaging framework, which consists of:

- the processing model that defines the rules for processing a SOAP message
- the extensibility model that defines the concepts of SOAP features and modules
- the underlying protocol binding framework describing the rules for defining a binding to an underlying protocol that can be used for exchanging SOAP messages between nodes
- the message construct defining the structure of a SOAP message

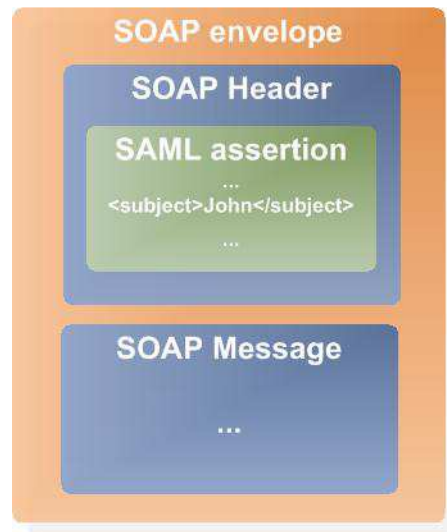


Figure 8: example of SOAP envelope

6.2.1.2 Web services security

Web Services Security (WS-Security or WSS) defines the basic mechanisms for providing secure messaging. It is an extension to SOAP that applies security to web services. In practice WSS makes it possible to prevent an eavesdropper or some third party from reading sensitive information that is transferred from one party to another. The SOAP specification provides a means for adding some security information to an individual message and WSS defines the information content in order to maintain security.

6.2.1.3 WS-Trust

The Web Services Trust Language (WS-Trust) is an OASIS standard that uses the secure messaging mechanisms defined by Web Services Security (WS-Security, WSS) in order to define additional primitives and extensions for the issuance, exchange and validation of security tokens. WS-Trust also enables the issuance and dissemination of credentials within different trust domains. In practice WS-Trust is an extension to WSS that deals with security token issuing, renewal and validation and relationship management in secure message exchange. The current version of WS-Trust is 1.4 and it was published in 2009.

6.2.1.4 PKI

Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures that are needed to:

- create,
- manage,
- distribute,
- use,
- store,

- revoke digital certificates.

In cryptography, a PKI is considered to be an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each certificate authority domain. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a certificate authority, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). For each user, the user identity, the public key, their binding, validity conditions and other attributes are made non-forgable in public key certificates issued by the CA.

6.2.1.5 X.509

The X.509 is an ITU-T standard for a public key infrastructure (PKI) for single sign-on (SSO) and Privilege Management Infrastructure (PMI). X.509 specifies standard formats for public key certificates, certificate revocation lists (CRL), attribute certificates, and a certification path validation algorithm.

X.509 was published in 1988 and is in association with the X.500 standard. It defines a strict hierarchical system of certificate authorities (CAs) for issuing the certificates which differs much from the web of trust model of e.g. PGP. X.509V3 includes the flexibility to support other topologies like bridges and meshes that can be used in a peer-to-peer, OpenPGP-like web of trust. The X.500 system has never been fully implemented, and the IETF's Public-Key Infrastructure (X.509), or PKIX, working group has adapted the standard to the more flexible organization of the Internet.

6.2.2 IAM languages

6.2.2.1 SAML

The Security Assertion Markup Language (SAML) was developed by the Security Services Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS). It is an XML-based framework that is used to communicate user authentication, entitlement and attribute information between an identity provider and a service provider. SAML enables business entities to make assertions regarding the identity, attributes and entitlements of a subject (human user or other entity) to other entities (company, enterprise application) thus enabling the use of single-sign-on (SSO) within an individual service. SAML is a flexible and extensible protocol designed to be used by other standards and has already been adopted among others by the Liberty Alliance and the Internet 2 Shibboleth project.

SAML V1.0 that became an OASIS standard in 2002, was followed by V1.1 in 2003 has been broadly implemented by Web access management vendors in the government and higher education, but also financial services and other industry segments. SAML V2.0 became an OASIS standard in 2005 and introduced features derived from the Liberty Alliance Identity Federation Framework (ID-FF) V1.2 specifications, and Shibboleth project, that enabled convergence for federated identity standards.

6.2.2.2 XACML

The eXtensible Access Control Markup Language (XACML) was developed by the Organization for the Advancement of Structured Information Standards (OASIS). It is a declarative access control policy language implemented in XML that includes a processing model describing how to interpret the policies. XACML V1.0 became an OASIS standard in 2003 and was superseded by V2.0 in 2005. XACML V2.0 introduced among others new profiles, such as (digital signature, multiple and hierarchical resources, role-based access control, security assertion markup language and privacy), enabled combination of algorithm parameters, as well as had an improved syntax in order to help implementation of the language.

The most recent version, XACML V3.0 was initially released in 2009 but not yet approved as a standard and therefore only a working draft. It introduces generic attribute categories for the evaluation context as well as an implementation of a new delegation mechanism that is used to support the decentralized administration of access policies. This means in practice that an authority may delegate all or parts of its own authority or even someone else's authority to a third party without the need to involve modification of the root policy.

XACML is divided into 3 levels of elements:

- PolicySet: a PolicySet contains one or more policies.
- Policy: a Policy contains one or more rules.
- Rule: a rule is a condition using subjects, resources and Actions.

Example of XACML access control rules:

Allow access
To **Secure Virtual Workspace** with attribute **Cloud access**
If subject is **Trauma Leader** and action is **read**

6.2.2.3 SecPAL

policy language for addressing complex access control requirements for decentralized systems. It is flexible and robust and developed especially for large-scale distributed computing environments. SecPAL V1.0 was introduced by Microsoft in 2007. SecPAL has been designed to support advanced requirements, for example:

- (un)constrained delegation of rights
- establishing trust within and across organizational boundaries
- distributed policy authoring and composition with enforced separation of duties
- fine-grained revocation
- cryptographically strong, Internet scale authentication information

The fundamental SecPAL concept is the security assertion that is a statement made by a principal that may:

- define a connection between a principal and an attribute
- specify the principal's permissions to operate on a specific resource

- express a trust or delegation
- express an authorization policy
- revoke a previous assertion
- declare principal identifier alias relationships

The assertions are made using uniform grammar that includes both a human (plain English sentences) and a machine (XML schema) version.

6.2.2.4 XrML

The eXtensible Rights Markup Language (XrML) was developed by ContentGuard and is based on the former Digital Property Rights Language (DPRL) developed by Xerox. XrML is based on an XML grammar and specifies rights and conditions with the objective of controlling the access to digital content and services. XMRL V1.0 was published in 2001 and followed by V2.0 in 2003. XrML enables the owner or distributor of digital resources (software or content) to identify the parties that are allowed access to these resources. In addition XrML provides information related to the rights as well as the terms and conditions related to the usage of the rights.

The current 2.0 version of the XrML message consists of the following four entities and their relationships:

- identity of the subject (target of the XrML grant)
- specification of the right
- definition of the object (resource that is the object of the right)
- condition for the right to be exercised

6.3 User provisioning

User provisioning objective is to create, maintain and delete user objects, attributes and rights in all systems, directories and applications.

6.3.1 SPML

The Service Provisioning Markup Language (SPML), is an XML-based standard developed by OASIS for exchanging provisioning information between systems. The first version 1.0 was approved in October 2003, and version 2.0 was approved in April 2006.

SPML defined 3 main actors:

- The requesting authority (RA) is the entity that makes a request
- The Provisioning Service Provider (PSP) is the entity that responds to the requests

The Provisioning Service Target (PST) is the entity that performs the provisioning
SPML version 2.0 functions could be divided into 9 categories:

- Core functions: main functions to add, delete, view, list or modify an object, or a list of objects
- Asynchronous capability: functions to cancel or get the status of an asynchronous request
- Batch capability: function to execute batch operation

- Bulk capability: functions to run multiple requests together
- Password capability: functions to manipulate the password of an object
- Search capability: functions for search operation
- Suspend capability: functions to suspend or resume an operation
- Update capability: functions for update capabilities
- Custom capability: this category is for some provider's specific functions implementation

This standard supports a lot of provisioning operation, and is supported by most provisioning tools, but few targeted systems implements this standard.

6.3.2 SCIM

The System for Cross-domain Identity Management (SCIM) specification was developed to manage user identities in cloud-based applications and services. It aims at provide a common user schema and extension model. The first version was released in December 2011, version 1.1 was releases in July 2012 to clarified some issues found during interoperability testing. The next version (2.0), is currently under development by the SCIM working group under IETF.

SCIM is built on several objects:

- Resource
- Schema
- ServiceProviderConfig
- CoreResource
- Group
- User
- EnterpriseUser

SCIM provides a REST API with a simple set of operations to create, read, replace, delete, update, search and bulk an object.

The initiative was driven by Google, Salesforce.com and Ping Identity to overcome the low level of adoption of SPML.

7 Transmission services

This section describes the main protocol and solutions for secured transmission services. First, we will have an overview of VPN technology and protocols, and then, we will present some typical use cases with VPN solutions. After that, we will have a quick overview of solutions for bandwidth optimization.

1.1 Secure transmission services

7.1.1 Secure sockets layer and Transport layer security

Secure Sockets Layer (SSL) is a cryptographic protocol that provides security for communications over networks such as the Internet. SSL was originally developed by Netscape that published V2.0 in 1995 and was followed by SSL V3.0 in 1996.

SSL and its descendant Transport Layer Security (TLS) encrypt the segments of network connections at the application layer to ensure secure end-to-end transit at the Transport Layer. TLS V1.0 was defined in RFC 2246 in 1999 as an upgrade to SSL V3.0. It was followed by TLS V1.1 in 2006 that included added protection against Cipher block chaining (CBC) attacks and support for IANA registration of parameters. TLS V1.2 was published in 2008 and introduced changes in the hash algorithms, an enhancement in the client-server abilities to specify which hash and signature algorithms they will accept and an expansion of support for authenticated encryption ciphers.

7.1.2 IPSEC protocol description

7.1.2.1 IPSEC Protocol Overview

IPSec, short for Internet Protocol Security, is a suite of protocols, standards, and algorithms to secure traffic over an untrusted network, such as the Internet. These services and protocols combine to provide various types of protection. Since IPSec works at the IP layer, it can provide these protections for any higher layer TCP/IP application or protocol without the need for additional security methods, which is a major strength.

IPSec provides four core services:

- Confidentiality – prevents the theft of data, using encryption.
- Integrity – ensures that data is not tampered or altered, using a hashing algorithm.
- Authentication – confirms the identity of the host sending data, using pre-shared keys or a Certificate Authority (CA).
- Anti-replay – prevents duplication of encrypted packets, by assigning a unique sequencing number.

The IPSec standard is outlined in RFC 2401.

A common use of IPSEC is the construction of a Virtual Private Network (VPN), where multiple segments of a private network are linked over a public network using encrypted tunnels. This allows applications on the private network to communicate

securely without any local cryptographic support, since the VPN routers perform the encryption and decryption.

IPsec is a group of protocols used on top of IP for the purpose of authentication, encryption and secure exchange of encryption keys.

The initial and main protocol is the IKE (Internet Key Exchange, RFC 2409) protocol. Applied to IPSec, the protocol aims to initially establish a first tunnel between two machines (IKE tunnel), that can be termed "administrative tunnel."

This is Phase 1 of the IKE protocol. This protocol is called Administrative because it is not used for the transmission of user data and is used to manage side tunnels, their creation, the refresh key, etc.

Phase 2 IKE is indeed to establish as many side tunnels as necessary for the transmission of user data between the 2 machines.

Tunnels for data exchange will be based on two different protocols depending on users' security needs.

The first is the AH (Authentication Header, RFC 2402) which aims to establish the identity of the end for sure. It does not guarantee any confidentiality (encryption) of data.

The second protocol is ESP (Encapsulating Security Payload, RFC 2406) protocol to encrypt data, with or without the packet headers (depending on the mode used). It also guarantees the authenticity of the data.

These two protocols, AH and ESP, on the other hand can be used separately or in combination.

7.1.2.2 Security Associations (SA)

IPSec introduces the concept of the Security Association (SA). An SA is a logical connection between two devices transferring data. An SA provides data protection for unidirectional traffic by using the defined IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

The SAs allow an enterprise to control exactly what resources may communicate securely, according to security policy. To do this an enterprise can set up multiple SAs to enable multiple secure VPNs, as well as define SAs within the VPN to support different departments and business partners.

7.1.2.3 IKE and IPSec Security Associations

IPSEC VPN peers establish a Security Association (SA), a "connection" between the two endpoints of the VPN tunnel.

Before the SA can be established, several parameters must be negotiated between VPN peers, and keys must be both created and exchanged. The Internet Key Exchange (IKE) protocol controls this negotiation process on UDP port 500.

IKE Policy Sets are created to negotiate several parameters, including:

- The encryption algorithm (such as DES, 3DES, or AES)
- The hashing algorithm (such as MD5 or SHA-1)

- The authentication method (such as shared keys or RSA signatures)
- The Diffie-Hellman (D-H) group for creating and sharing keys
- The SA Lifetime, measured in seconds or in kilobytes sent

During the negotiation process, VPN peers share their list of configured IKE policies. The SA will only be established if there is an exact matching policy between the peers.

There are two phases to this negotiation process:

IKE Phase 1 establishes the initial tunnel (referred to as the IKE SA). Peers are authenticated, encryption and hashing algorithms are negotiated, and keys are exchanged based on the IKE Policy Sets.

IKE Phase 2 establishes the IPSec tunnel (IPSec SA), which details the AH or ESP parameters for securing data.

IKE Phase 1 negotiates parameters for the tunnel (key exchange) itself, while IKE Phase 2 negotiates parameters for the data traversing that tunnel.

7.1.2.4 Key Management

IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it.

IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process of refreshing keys; however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

7.1.2.5 The authentication protocol AH

The ESP (Encapsulating Security Payload) protocol provides the following security services:

- Integrity
- Authentication data
- Anti-replay (optional)

The authentication header is inserted into the packet between the IP header and any subsequent packet contents. The payload is not touched.

Although AH protects the packet's origin, destination, and contents from being tampered, the identity of the sender and receiver is known. In addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read.

ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following figure, IP HDR represents the IP header and includes both source and destination IP addresses.

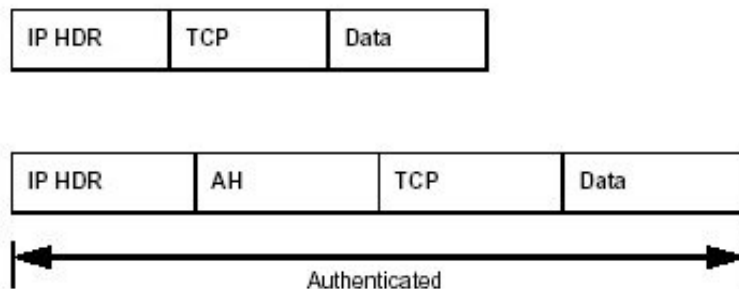


Figure 9: packet with AH

7.1.2.6 The confidentiality protocol ESP

The ESP (Encapsulating Security Payload) protocol provides the following security services:

- Privacy
- Protection against traffic analysis
- Integrity (as AH)
- Authentication data (such as AH)
- Anti-replay (as AH)

ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.

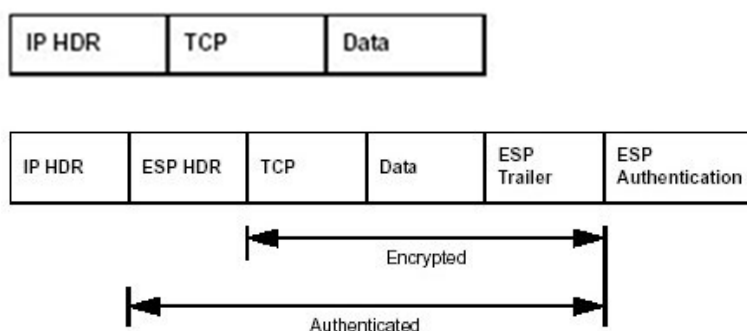


Figure 10: packet with ESP

7.1.2.7 Description of IPSec modes

A mode is the method in which the IPSec protocol is applied to the packet. IPSec can be used in tunnel mode or transport mode:

7.1.2.7.1 Transport Mode

Protection is provided for the data in the IP packet through encryption but not for the IP header information, which remains unchanged. Transport Mode adds only a few bytes of information to each IP packet, in the form of an IPSec header, and it allows for quality-of-service (QoS) management on the network. Transport Mode is typically used when end-to-end encryption is required and supported by the peers and is deployed between or within locations.

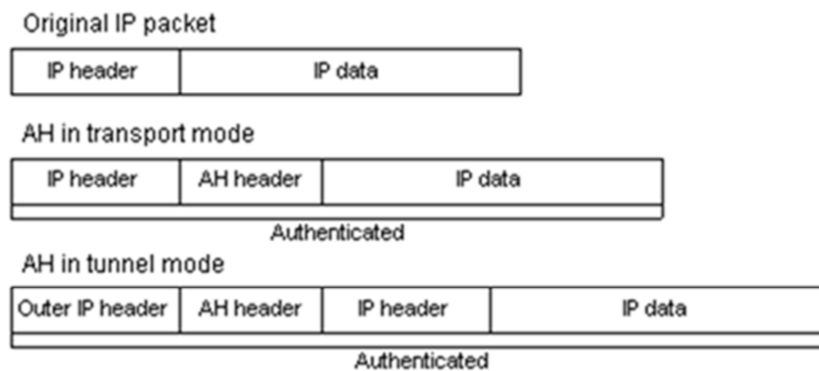


Figure 11: IPSEC packet with AH

7.1.2.7.2 Tunnel Mode

Protection is provided for the entire IP packet, which is encrypted and then encapsulated in a new IP packet including a new IP header and an IPSec header.

Tunnel Mode is typically used on IPSec gateway devices such as firewalls, routers, and VPN appliances connecting remote locations such as branch offices. The gateway acts as an IPSec proxy for the clients that are located behind the device. Clients forward IP packets to the gateway in the clear. The gateway device then encrypts the packet and forwards it to an IPSec peer, which in turn decrypts the packet and forwards it to the destination client.

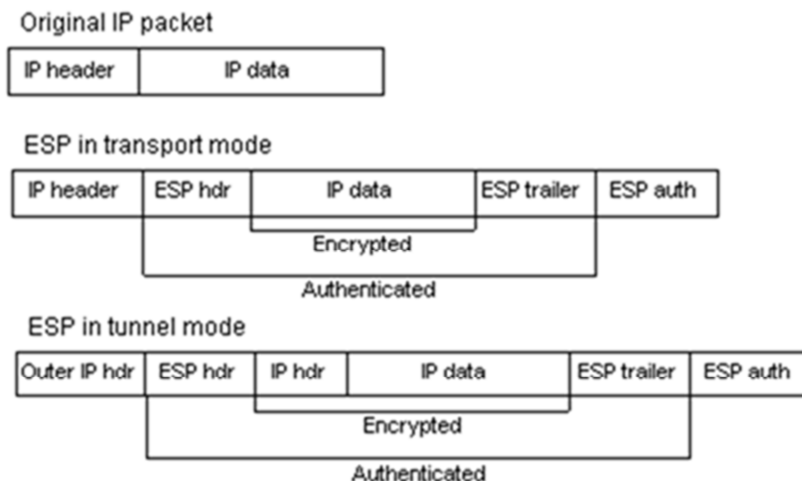


Figure 12: IPSEC packet with AH and ESP

7.1.2.8 Transport vs. Tunnel Modes

Each IPsec protocol (AH or ESP) can operate in one of two modes:

- Transport mode – Original IP headers are left intact. Used when securing communication from one device to another single device.
- Tunnel mode – the entire original packet is hashed and/or encrypted, including both the payload and any original headers. A temporary IP header is applied to the packet during transit. Used to tunnel traffic from one site to another

7.1.3 Virtual Private Networks (VPNs)

A Virtual Private Network (VPN) provides a secure tunnel across a public (and thus, insecure) network. This provides a mechanism for organizations to connect users and offices together, without the high costs of dedicated leased lines.

VPNs are generally used for two purposes:

- Site-to-Site VPNs - connect remote offices to a main office.
- Client VPNs - connect home or “roaming” users to an office.

7.1.3.1 Site-to-Site VPN

A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world.

There are two types of site-to-site VPNs:

- Intranet-based -- If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect each separate LAN to a single WAN.
- Extranet-based -- When a company has a close relationship with another company (such as a partner, supplier or customer), it can build an extranet VPN that connects those companies' LANs. This extranet VPN allows the companies to work together in a secure, shared network environment while preventing access to their separate intranets.

7.1.3.2 Client or remote access VPN

Most traditional VPN solutions follow the client-server principle, which means that all participating nodes connect to a central server. This creates a star topology, which has some disadvantages. The central node needs lots of bandwidth, because it needs to handle all the VPN traffic. Also, if the central node goes down, the whole VPN is down too.

A remote-access VPN allows individual users to establish secure connections with a remote computer network. Those users can access the secure resources on that network as if they were directly plugged in to the network's servers. An example of a company that needs a remote-access VPN is a large firm with hundreds of salespeople in the field.

There are two types of remote access VPNs: IPSec and SSL.

7.1.3.3 Remote Access IPSec VPNs

Remote access IPSec VPNs permit secure, encrypted connections between a company's private network and remote users, by establishing an encrypted IPSec tunnel across the Internet using broadband cable, DSL, dial-up, or other connections.

A remote access IPSec VPN consists of a VPN client and a VPN gateway. The VPN client software resides on a user's workstation and initiates the VPN tunnel access to the corporate network. At the other end of the VPN tunnel is the VPN gateway at the edge of the corporate site.

When a VPN client initiates a connection to the VPN gateway device, negotiation consists of authenticating the device through Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth). Next the group profile is pushed to the VPN client using mode configuration, and an IPSec security association (SA) is created to complete the VPN connection.

The biggest benefit of IPSec is that because it operates at the IP layer it provides a lot of flexibility with respect to network configurations and applications. It means that traditional legacy applications can be accessed easily and simply without the need for major development and reconfiguration, using the respective clients.

7.1.3.3.1 Remote Access SSL VPNs

An SSL VPN lets users to access enterprise networks from any Internet-enabled location. Users can make clientless connections, which use only a Web browser that natively supports Secure Socket Layer (SSL) encryption.

User authentication can be done using usernames and passwords, certificates, or both.

The primary benefit of an SSL based remote access VPN solution is that there is no client required necessarily. For web-enabled applications a simple HTTPS connection to the web server is all that is required to access those services.

7.1.3.4 Peer-to-peer VPN

A peer-to-peer VPN builds virtual networks between multiple computers. Such a virtual network can be useful to facilitate direct communication that applications like file sharing or gaming may need.

A peer-to-peer (P2P) network comprises equally privileged participants. No participants are clearly servers or clients in the communication. They both provide and consume resources.

Several VPN peer-to-peer products are proposed. Their cryptographic module is software implemented. A step beyond would be the use of a hardware cryptographic module for secure key storage.

7.2 Dependable transmission services

7.2.1 Infiniband

InfiniBand is a type of communications link for data flow between processors and I/O devices that offers throughput of up to 2.5 gigabytes per second and support for up to 64,000 addressable devices. Because it is also scalable and supports quality of service (QoS) and failover, InfiniBand is often used as a server connect in high-performance computing (HPC) environments.

The internal data flow system in most PCs and server systems is inflexible and relatively slow. As the amount of data coming into and flowing between components in the computer increases, the existing bus system becomes a bottleneck. Instead of sending data in parallel (typically 32 bits at a time, but in some computers 64 bits) across the backplane bus, InfiniBand specifies a serial (bit-at-a-time) bus. Fewer pins and other electrical connections are required, saving manufacturing cost and improving reliability. The serial bus can carry multiple channels of data at the same time in a multiplexing signal. InfiniBand also supports multiple memory areas, each of which can be addressed by both processors and storage devices.

The InfiniBand Trade Association views the bus itself as a control information that determines the route a given message follows in getting to its destination address. InfiniBand uses Internet Protocol Version 6 (IPv6), which enables an almost limitless amount of device expansion.

With InfiniBand, data is transmitted in packets that together form a communication called a message. A message can be a remote direct memory access (RDMA) read or write operation, a channel send or receive message, a reversible transaction-based operation or a multicast transmission. Like the channel model many mainframe users are familiar with, all transmission begins or ends with a channel adapter. Each processor (your PC or a data center server, for example) has what is called a host channel adapter (HCA) and each peripheral device has a target channel adapter (TCA). These adapters can potentially exchange information that ensures security or work with a given Quality of Service level.

The InfiniBand specification was developed by merging two competing designs, Future I/O, developed by Compaq, IBM, and Hewlett-Packard, with Next Generation I/O, developed by Intel, Microsoft, and Sun Microsystems.

The figure Figure 13: using Infiniband depicts an example of network architecture where Infiniband is dedicated to business communications and a conventional network is reserved for administration.

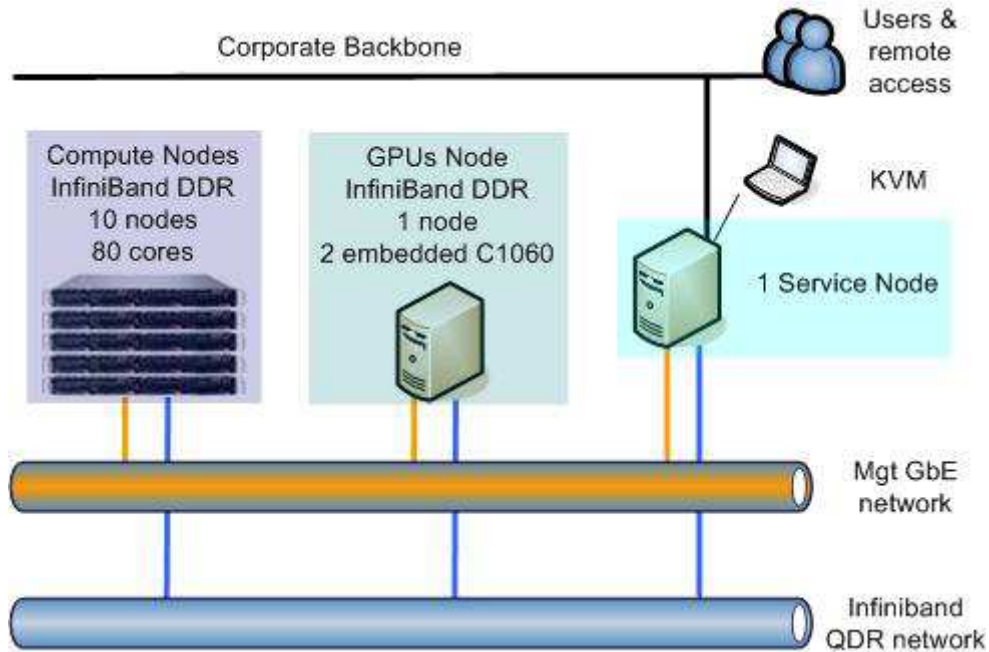


Figure 13: using Infiniband

The Figure 14 gives the global view of common Infiniband network architecture.

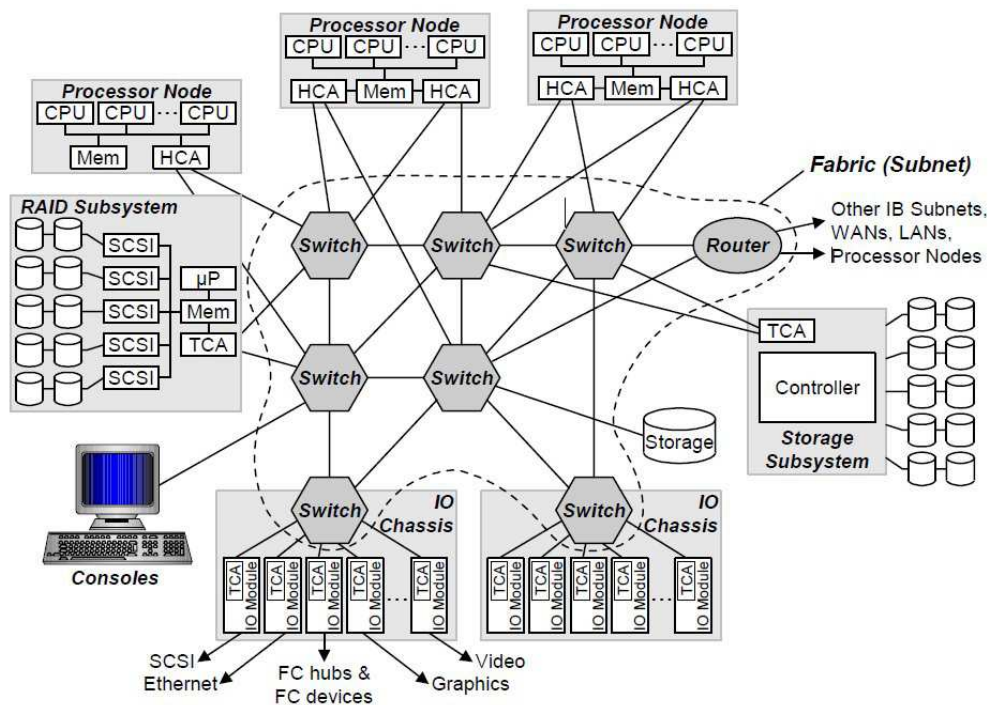


Figure 14: Common Infiniband network architecture

7.2.2 Protocol optimization

The Transport layer for a protocol stack is responsible for getting the message to the application on the destination machine. Generally TCP is used by many of the applications because it guarantees reliable delivery. Unfortunately, in reality parts of a message sometimes will not reach the destination or will reach the destination corrupted. Thus, TCP needs some means of detecting and recovering from lost or damaged message parts. This means of recovering from errors is called Reliable Data Transfer (RDT). The RDT is manifested in two protocols: Stop-and-Wait and Pipelined (Selective Repeat).

7.2.2.1 RDT protocols

Stop-and-Wait: The TCP protocol is based on the use of acknowledgements, timeouts, and retransmission. These protocols retransmit a data packet if acknowledgements and timeouts indicate that the data packet may not have been successfully transmitted during the previous attempt. In Stop-and-Wait the Sender sends one data packet. When the receiver receives that data packet, the receiver checks if the data packet has been corrupted. If the data packet has not been corrupted, then the receiver sends an acknowledgement packet back to the Sender. When the Sender receives the acknowledgement, the Sender can then send the next data packet.

Pipelined (Selective Repeat): In a pipelined reliable data transfer protocol, the sender can start sending a second data packet before the sender receives the acknowledgment for the first data packet. Thus, if the sender needs to send several packets, then the time until the last of the packets is sent will be shorter with a pipelined protocol. Thus, a pipelined protocol can have better performance than the Stop-and-Wait protocol.

7.2.2.2 RDT formats

MPEG-4 AVC (Advanced Video Coding) standard developed by the ITU-T Video Coding Experts Group (VCEG) together with the ISO/IEC JTC1 Moving Picture Experts Group (MPEG). AVC streams are configured using parameter sets. There are two types of parameter sets: Sequence Parameter Set (SPS) and Picture Parameter Set (PPS). An active sequence parameter set remains unchanged throughout a coded video sequence, and an active picture parameter set remains unchanged within a coded picture. The sequence and picture parameter set structures contain information such as picture size, optional coding modes employed, and macro-block to slice group map.

MPEG-4 Binary Format for Scenes (BIFS) published as ISO/IEC 14496-11 MPEG-4 Part 11, is a binary format for composition of MPEG-4 objects, user interaction and its animation. It follows an object-oriented and a stream-based design. All presentations are described in a scene-graph, which is a hierarchical representation of audio, video and graphical objects, each represented by a node abstracting the interfaces to those objects. This allows manipulation of an object's properties, independent of the object media, where the scene-graph structure allows high level description of the presentation and makes the coding of media independent (e.g. video, images, audio,

etc...). It also gives a well-defined framework for building up interaction between elements and dealing with user-input (e.g. TouchSensor, InputSensor).

MPEG-4 Lightweight Application Scene Representation (LAsER) published as ISO/IEC 14496-20 MPEG-4 Part 20, is a binary specification designed for representing and delivering rich-media services to resource-constrained devices such as mobile phone. A rich-media service is a dynamic and interactive presentation comprising 2D vector graphics, images, text and audiovisual material. The representation of such a presentation includes describing the spatial and temporal organization of its different elements as well as its possible interactions and animations.

MPEG User Description (MPEG-UD) is a new specification (i.e. description) of a standard aiming to ensure interoperability among recommendation services, which take into account the user and its context. In order to achieve interoperability, the MPEG-UD provides a standard description of User, Context and Services. The applications (run by the user or service provider) used to respond to user's request consume a standard representation of the recommendation. The Recommendation Description (RD) as an input format to the application is composed not only of subsets from UD/CD/SD, but also of additional logical relations and metadata related to the subsets.

Standard	Type of data	Advantages	Disadvantages
MPEG-4 AVC	video, audio	<ul style="list-style-type: none"> • gain in bit rate by half compared to MPEG-2 • deployed for Digital Multimedia Broad casting & HDTV • support of different profiles 	<ul style="list-style-type: none"> • complex implementation • single CPU processing
MPEG-4 BIFS	text, graphics, image, 2D/2D+t0, 3D, audio, video	<ul style="list-style-type: none"> • hierarchical audio-visual object representation • full multimedia 2D/3D support • direct collaborative interaction with audio-visual objects 	complex scene-graph management
MPEG-4 LASER	text, graphics, image, 2D/2D+t0, audio, video	<ul style="list-style-type: none"> • easy implementation • rich-media services for smartphones & tablets 	limited to 2D visual object representation
MPEG-UD	XML schema, RDF schema, Ontologies	<ul style="list-style-type: none"> • interoperability among users, contexts and services • standard recommendation format 	complex big data configurations

Table 3: RDT formats summary

8 Fingerprinting and watermarking

This section presents two solutions to protect data. First, we will define Watermarking, and its application for medical imaging, then, we will present fingerprinting in medical applications.

References of this section are available in Appendix 1: Fingerprinting & Watermarking references

8.1 Watermarking in a nutshell

8.1.1 Definition

Digital watermarking can be defined as the process of embedding a pattern of information into a cover digital content (image, audio, video, etc.) [COX 02] [MIT 09]. The insertion of the mark is always controlled by some secret information referred to as a key. The subsequent watermark detection can serve to a large variety of applications, from property and/or integrity proof to augmented reality. Once watermarked, the host data can be transmitted and/or stored in a hostile environment, i.e. in an environment where changes attempting to remove the watermark are likely to occur.

While the key should be kept secret (i.e. known only by the owner), the embedded information and even the embedding method can be public.

There are no universal requirements to be satisfied by all watermarking applications. Nevertheless, some general directions can be given for most of the applications. In order to be effective, the watermark should be perceptually invisible for a human observer (transparency) and its detection should be successful even when the watermarked content is attacked (robustness). Moreover, it should allow the insertion of a sufficient amount of information (data payload) required by the targeted application (e.g. a serial number identifying a user, a time stamp, etc.). The definitions for these general properties, as well for some additional practical features, are detailed below.

8.1.2 Watermark criteria

8.1.2.1 Transparency

The notion of transparency is related to the perception (visual, auditory ...) of artifacts resulted from the insertion process. Watermarking should be imperceptible and invisible to a human observer (the embedded watermark should not affect the quality of the host data).

The visual quality assessment of the watermarked data remains an important criterion for validating the watermarking algorithm. However, it is a subjective concept that depends on various criteria: human visual system, age, experience, artistic sense, observation condition. Thus, it is complicated to evaluate whether a watermarking method is transparent or not. Such an evaluation requires significant testing involving a wide observer's panel and many visual assessments [MAN 74]. An alternative is the use of objective transparency metrics.

An objective measure is a function that takes as input some video information, calculates the distance to some reference information extracted from reference video

and outputs a value somewhat associated to that differences. Based on the way they act, objective measures can be classified into three classes [AVC 01]:

- **Pixels difference measures** are based on differences between the original and the modified image. The signal to noise ratio (PSNR), the maximum mean square error (PMSE), the image fidelity (IF) and the average absolute difference (AAD) are the most common, due to their easily use and implementation.
- **Correlation measures** reflect the similarity between two images even in the presence of a low noise compared to the pixel strength, such as the normalized cross correlation (NCC), the correlation quality (CQ) and the structural content (SC) belong to this class.
- **Psychovisual measures** consider the human visual system as a spatio-temporal filter. For the instance, the digital video quality (DVQ) models the human visual system according to luminance intensity, frequency contents and structural content.

In some watermarking applications, the perceived quality needs to be ultimately evaluated using subjective assessment measures. However, since this measurement type requires a sizable panel of observers and carefully controlled environment, they are both time-consuming and expensive. On the other hand, subjective testing is the most reliable methodology allowing evaluating the human quality perception of artifacts induced in images. The international Standard organization (ISO) introduced in 2004 [KEE 04] the ISO 20462 for psychophysical image quality measurement. The standard presents two methodologies, the triplet comparison and the Quality Rule to be used for measurement over small and wider range of quality respectively. Of course, the International Telecommunication Union describes other methods for subjective quality assessments [BT 98] [BT 02]. The Double-Stimulus Continuous Quality-Scale (DSCQS), the Double-Stimulus Impairment Scale (DSIS) and the Single Stimulus for Continuous Quality Evaluation (SSCQE) can be considered.

8.1.2.2 Robustness

Robustness is the ability of the mark to survive changes undergone by the host media. These changes (be they intentional or unintentional) define the set of attacks. The various possible attacks against watermarked video can be structured into four classes [PET 98], according to the way they act: removal attacks, geometric attacks, cryptographic attacks, and protocol attacks.

The removal attacks try to make the watermark unreadable. This class includes attacks by noise addition, denoising, transcoding quantization, ...

The geometric attacks aim to destroy the synchronization of the watermark. After such an attack, the watermark is still present in the video, but its location is unknown at the decoder. Rotations, curvatures, jitter of pixels individually considered or combined into the Stirmark attacks, fall into this category [PET 98].

Protocol attacks aim to make watermark unusable by creating some ambiguities concerning the mark usage. Attacks by inversion and copy belong to this class. The former creates a false key so that by applying the detection procedure, the watermark indicates a different owner for the video.

The cryptographic attacks try to manage the watermark (detect/copy/insert a new one) without knowledge of the secret key. One example is represented by the brute-force search. Another example, known as the oracle attack, consists in creating an unmarked version of the signal by exploiting the response of a detector (assuming it is available). In any case, this type of attack is very restrictive in practice because of its complexity.

8.1.2.3 Fragility and semi-fragility

A watermark system is fragile to an attack when the watermark cannot be detected after slightest modifications generated by this attack.

A watermarking system is semi-fragile when both particular robustness and fragility properties are imposed to the system. Once the classes of allowed and non-allowed attacks have been defined based on the targeted application, the watermark must survive all manipulation belonging in the former class (the robustness), but it should be destroyed by the manipulations belonging to the latter (the fragility).

The required degree of each requirement presented above depends on the watermarking application. A watermarking application is effective when ensures the functional balance of the three requirement degrees of transparency, robustness, data payload. However, some applications can require additional features, like cost minimization, constant bit-rate, format compliance, etc.

8.1.2.4 Data payload

This is the total amount of information (in bits) inserted into original content. According to the targeted applications, the specifications on this factor may be very different, from 64 bits per sequence for the identification of ownership up to hundred of kilobits per frame for application of hyper-video

8.1.2.5 Cost

The technical cost of the algorithm is also significant feature of any watermarking method. From this point of view, the complexity of the algorithm is the main criterion of practical acceptance.

8.1.2.6 Constant bit-rate

Watermarking method should not increase the size of the compressed data and the bit-rate, at least for constant bit-rate applications where the transmission channel has to be obeyed.

8.1.3 Theoretical model

From the structural point of view, any watermarking procedure features three components: the watermark generation (i.e. the way in which the message to be inserted is encrypted with a secret key so as to obtain a watermark), the watermark embedding (i.e. the way in which the watermark is inserted in the host document) and the watermark detection (i.e. the way in which the watermark is recovered).

From the information theory point of view, the watermarking process can be considered as a communication system with side-information at the encoder, see Figure 1. Using a secret key k , the watermark message m is embedded into the host signal x . The watermarked signal s is then transmitted over the channel which can

introduce a noise n resulting from the attacks. The decoder receives the signal r and, using the same key k , extracts the watermark message m' .

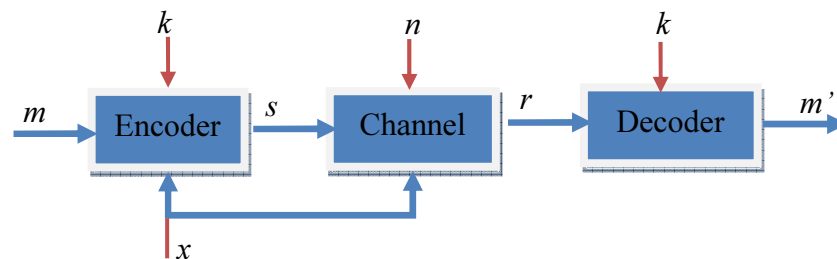


Figure 8: Watermarking synopsis diagram.

8.1.4 Watermarking application

Watermarking techniques have been deployed in several applications. The 3 main applications are illustrated in Table 3. For a more thorough investigation we can refer to [DOE 03, BAR 01].

Applications	Purpose
Copyright protection	Proof of ownership
Video authentication	Detect that the original content has been altered or not
Video enrichment	Enhance video content and make it more interactive

Table 4: applications and purposes

Copyright protection: For the protection of intellectual property, the video data owner can embed a watermark representing copyright information in his data. Thus, watermarks provides owner identification (by embedding the identity of videos' copyright holder), proof of ownership (by providing evidence in ownership dispute), transaction tracking (by identifying people who obtain content legally but illegally redistribute it). This type of application requires a maximum strength of robustness.

Video authentication: With the ease of visual data modification in the digital domain, unauthorized alterations could be made without any perceptible trace. Consequently, the video recorded by a video surveillance system has no value as evidence in court unless the integrity can be verified. This type of application requires robustness against mundane video processing operations but fragility against malicious modification attacks. Watermarks embed signature information in content that can be later checked to verify it has not been tampered with.

Video enrichment: Watermarking can be useful for video enrichment applications. At any time viewing, the user can click on an element of the video to extract information that has already been embedded about that item. This type of application usually requires the insertion of a large amount of information compared to the rest of the conventional video applications.

8.1.5 Watermarking classification

Watermarking techniques can be divided into different categories according to various criterions [LEE 01]. The general classification of the currently available watermarks is shown in Figure 2.

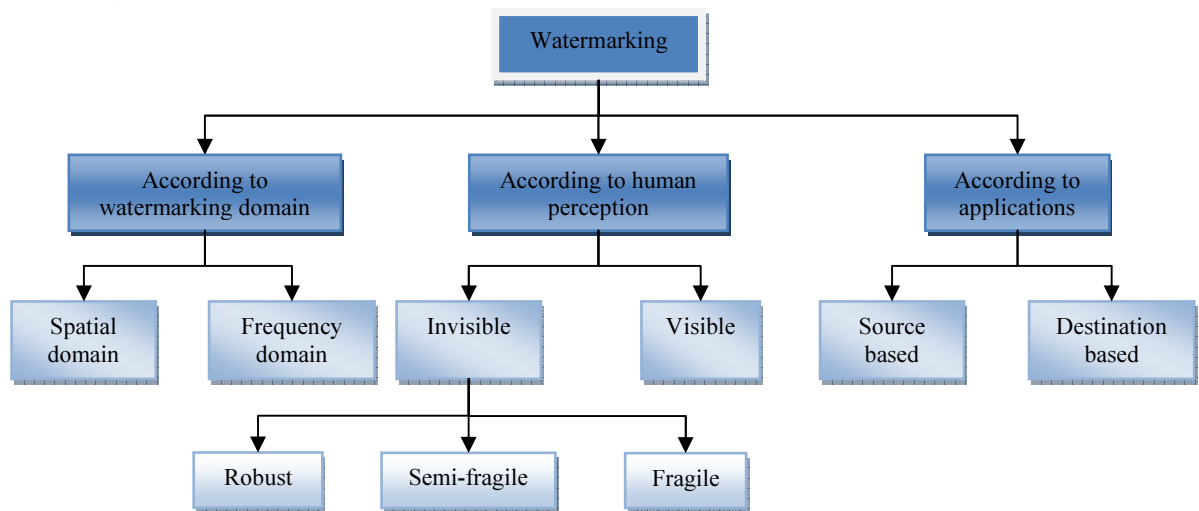


Figure 15: watermarking classification diagram

Watermarking techniques can be classified into different categories according to several criteria [COX 01]. In this Section we will expand two classification strategies, based on the type of the domain in which the data embedding takes place and based on the robustness of the mark to attacks.

In terms of the domain in which the watermark is inserted, watermarking system can be classified as spatial-domain, transform-domain or compressed-domain watermarking algorithms [COX 01], [SON 09].

In spatial domain systems, the watermark is inserted directly in the pixel domain. Many of spatial watermarking techniques provide simple and effective schemes for embedding an invisible watermark into an image, but are less robust to common attacks. Watermarking schemes in the spatial domain are generally less robust towards noise-like attacks such as lossy JPEG compression. However the big advantage is that the watermark may easily recovered if the image has been cropped or translated.

In the transform domain watermarking systems, watermark insertion is done by transforming the image into some frequency domain, by using a given transform: Discrete Fourier Transform (DFT), full-image DCT (Discrete Cosine Transform), block-wise DCT, etc. It is often claimed that embedding in the transform domain is advantageous in terms of visibility. Designing watermarking algorithms in the transform domain is not as simple as in the spatial domain. However, there are many

DCT-domain algorithms, because this transform is involved in many compression standards such as JPEG, MPEG-2, H.263 or MPEG-4 AVC, for instance.

Since video signals are usually stored and distributed in a compressed format, it is often impractical to first decode the video sequence, embed the watermark, and then re-encode it. Thus, designing low-complexity video watermarking algorithms in the compressed domain is attractive.

In terms of their robustness to attacks, watermarking technique can be classified as fragile, robust and semi-fragile [SER 02].

With the aim of detecting the tampering of the original content, fragile watermarking techniques should not survive lossy transformations applied on the watermarked content. Consequently, the watermark information is generally embedded into the perceptually insignificant portions of the data. From the applicative point of view, fragile watermarking is used to guarantee the content authenticity [LIN 99].

Robust watermarks must survive to intentional and non intentional alterations. For a watermark to be robust, the watermarks should be embedded into the significant portion of the content. Consequently, the technical challenge is to provide transparency and robustness, which are conflicting requirements. Robust watermarking is designed to provide proof of ownership of the media in question, thus serving IPR (Intellectual property rights) purposes and being suitable for DRM (Digital Right Management).

Semi-fragile watermarks should be insensitive to some common non malicious transformations, such as compression, but should be sensitive to image transformations that alter the content information, such as deleting or replacing a part of the image. When designing semi-fragile watermarking methods, the challenge is to provide tools able to distinguish between malicious and mundane video processing. Generally, semi-fragile watermarks are deployed for integrity verification applications.

8.2 Watermarking for medical imaging

This section specifies the peculiarity of the watermarking when applied to medical images.

8.2.1 Usefulness of watermarking in medical imaging

One of the major concerns throughout the world is to make high quality healthcare available to all. Part of difficulty in achieving equitable access to healthcare was been that healthcare service provider and recipient must be physically present in the same consulting area. However, advents in multimedia services and information communication technologies [KOL 99] have increased the number of ways in which healthcare can be delivered to reduce these difficulties.

Telemedicine, the area where medicine and information communication technology meet, is probably the main part of this advancement that may have the significant impact on healthcare delivery. The information infrastructure of modern healthcare is based on digital information management. Thus, boosted the potential of medical information handling and sharing with application ranging tediagnosis to telesurgery and collaborative working session.

While the recent advances in multimedia and information communication technologies offer new ways to access and handle medical images, they also compromise their security and integrity due to their ease of manipulation replication.

Because of the importance of security/protection issues in the management of medical information, it is mandatory to use watermarking technique to complete existing measures to protect medical images. Indeed, the security of medical information is derived from ethics and strict legislative rules. These latter gives the patient the rights to professional healthcare able to satisfy three mandatory features (see Figure 3): confidentiality, reliability and availability [GOA 00].

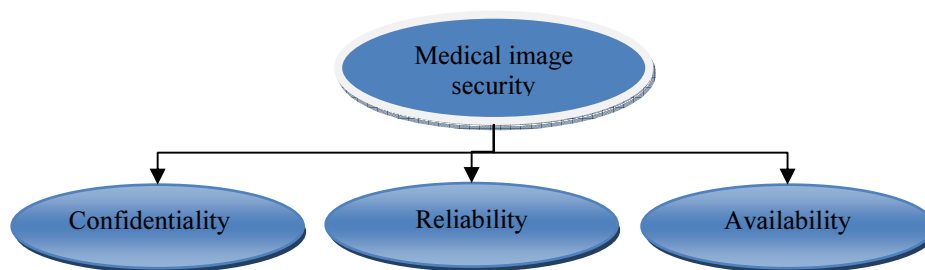


Figure 16: Medical images security properties

- **Confidentiality:** In normal required conditions, only authorized users have the access to the medical information.
- **Reliability:** This feature has two aspects. The first is connected to the information **integrity**. Consequently, the information must not be modified by non-authorized user and, conversely any non authorized modification must be detected. The second relies on the **authentication property**. Indeed, it must be verified that the medical information is coming from the right source and is belonging to the right patient.
- **Availability:** The ability of the information system to be used by authorized users under normal constraints for access and practices.

There are many current security tools commonly deployed to ensure each of the three properties. However they still have their own limitations. An overview of the security tools and of their limitation is presented Table 2 (For more details we can refer to [GOA 00]).

Security measurements	Limitations
Access control	may be broken or rapped
Digital signature	The signature and the information content are

	stored and transmitted separately.
Encryption	The encryption can change the hot information (very sensitive to bit error occurring during transmission).

Table 5: applications and purposes

Watermarking is designed to embed additional information which by construction is attached to the watermarked support. Watermarking techniques may be able to overcome the current limitations. The critical medical context states specific requirements that should be satisfied to reach the targeted medical application efficiency. These requirements are detailed in the following section.

8.2.2 Medical imaging watermarking requirements

Digital watermarking proposed for medical imaging is a special subset of image watermarking. That particularity is relied on the critical use of medical imaging in patient diagnosis. Consequently, watermarked medical images should not differ perceptually from their originals, in the sense that the watermarking technique should not bias the diagnosis in any way.

The purpose of fragile watermarking is to enhance medical imaging security, confidentiality and integrity while trying to preserve the image diagnosis quality and to avoid critical information loss.

8.2.3 Watermarking method for medical imaging

Generally, three main classes of watermarking method were identified for medical images [GOA 01].

A first class that includes methods that embed the mark within the region of non-interest (RONI) in order not to bias the diagnosis interpretation [SHI 05]. Various works suggest that RONI refer in general to black background of the image; however RONI can include gray level portion of little interest [MAC 99], hence leaves some more room for watermarking. Since there is no interference with interest medical image content, transparency is less strict; thus increase the method data payload. Despite, no interferences occur between the RONI and the data potentially used for the diagnosis, it has been shown that modifying black background by salt and pepper noisy pattern may bother medical interpretations. Therefore, the watermark information amplitude should be correctly set.

The second approach corresponds to reversible watermarking method. Once the embedded information is detected, the watermark is removed allowing the reconstruction of the original image [VLE 03]. Reversible methods are generally fragile and deployed for integrity verification application. Methods which tried to achieve high robustness level introduced in the image visible salt-and-peeper noise [MIA 00].

While reversible watermarking facilitates the watermark information updating, the resulting watermarked images remains unprotected and may be moved and replaced by other marks. In addition, the mark must be removed before any interpretation and it may cause additional time delay for physician.

The third approach consists in using jointly classical watermarking method and distortion minimization. In that case, the watermark replaces some image details by watermark information such as the least significant bit.

8.2.4 State of the art of medical imaging watermarking

Medical image watermarking was already the subject of several studies, see Table 3.

In [VEL 10], the authors advance a reversible blind watermarking system to watermark the medical image with the facial image of the patient in an invisible manner, in order to hide the identity of the patient in telediagnosis. Once the patient image is embedded in the covered image, the patient identity can be delivered to the authorized physicians by a key based extraction. Experiments result in transparency estimated at average PSNR around 35 dB. When the watermarked image is not the subject of attack, the extracted watermark is intact and the cover image is recovered completely without loss of details. An injection of Poisson noise results a degradation of the reconstructed images and the watermark.

S. Poonkuntran et al [POO 11] propose a reversible watermarking scheme for medical images (color fundus images). The embedding method includes two steps. First, a pixel set is selected according to the image color features. Secondly, the secret information is embedded by using the difference expanding method of the two pixels from different color planes. It is also found that 30000 bits is the optimum size of the watermark with good level of imperceptibility which is above 60 dB PSNR, in average. The paper does not include any robustness/fragility evaluation.

A watermarking scheme that can recover the original image from the watermarked one is advanced [JAS 07]. The issue is to verify the integrity and the authenticity of DICOM (Digital Imaging and Communication in Medicine) images (ultra sound images are experimented). SHA-256 of the hot image is embedded in the last non significant bit of the RONI. Further, the watermark will be extracted and the original image will be recovered. The SH1-256 of the recovered image will be compared with the extracted watermark in order to verify the image integrity. Experiments shown that a data payload of 510 kb is reached at transparency of PSNR around 31 dB. Also, the sensitivity to content changing (cloning an area of 50x50 pixels) is proved.

A binary mark carried out on the EPR (Electronic Patient Record) information is embedded into the DCT domain of RONI [KAU 13]. Experiments conducted under the medical image database proved that the mark degrades at around the same rate as degradation of the original image. Consequently, the EPR is recovered when the marked image is stored at JEPEG quality more than $Q = 30$. The transparency of the method is guaranteed by a PSNR more than 30 dB. However, the paper does not evaluate the integrity verification.

Pal et al present a novel scheme for biomedical image watermarking in wavelet domain [PAL 12]. A multiple copies of the watermark data is embedded in the cover using bit replacement in the horizontal and vertical resolution approximation image components. Experimental results show that the proposed scheme could embed a 16x16 logo while featuring a low level of distortion (around 40 dB). The method also proved its robustness against JPEG compression (95% of compression rate) and salt and pepper noise. Thus, a value of 0.76 and 0.79 of SSIM are obtained for JEPEG (5% of distortion) and salt and pepper noise (40%), respectively.

A RONI based watermark embedding is presented in [GUN 12]. A logo of 64x64 is embedded in the 3 level wavelet transform coefficients. The Experimented data base

resulted in a correlation factor for noise addition, filtering, compression, ranging from 0.9 to 0.95. A PSNR up to 48 dB is registered. However, the paper does not investigate the integrity verification performances.

In [MIA 00], the authors embed the EPR (Electronic Patient Record) data and the Doctor identity or the diagnostic report within the medical image by using a bipolar multiple base data hiding. The experiment results show that the distortion induced by embedding technique is no more than that induced by JPEG compression, reaching a PSNR more than 33 dB. The robustness/ fragility of the method has not been investigated.

Author	Type	Embedded data	Robustness/fragility	transparency
[VEL 10]	Reversible	Facial image of the patient	Fragile to poison noise addition	PSNR around 35 dB
[POO 11]	Reversible	Secret information (up to 30 000 bits)	NA	Average of 60 dB
[JAS 07]	Reversible RONI	SHA-256 of the image up to 510 kb	Sensitive to content alteration	31 dB of PSNR
[KAU 13]	RONI	EPR information	Robust against JPEG compression (QF=30)	More than 30 dB of PSNR
[PAL 12]	classical watermarking method	16x 16 logo	- Robust against JPEG compression - Robust against salt and peeper noise	40 dB of PSNR
[GUN 12]	RONI	64x64 logo	-Robust against compression (20%) - Robust against salt and peeper - Robust against median filtering	48 dB of PSNR
[MIA 00]	Classical watermarking method	The EPR data and the doctor identity or the diagnostic report	NA	PSNR more than 33 dB

Table 6: synopsis of the state of the art of medical imaging watermarking

8.3 Image fingerprinting in medical applications

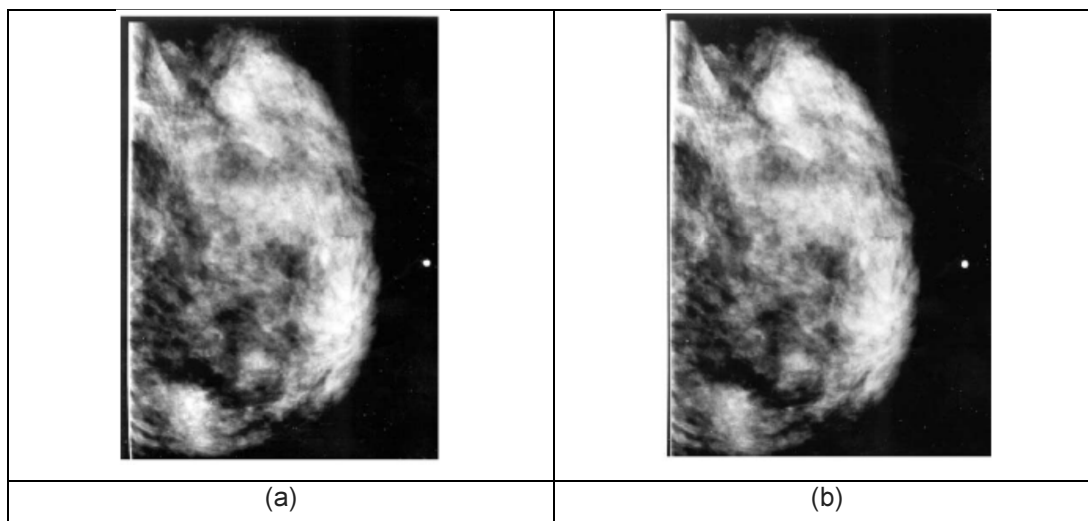
8.3.1 Introduction

The worldwide mass production context brings technology closer to people. Affordable capturing, processing and storage devices along with wide spread broadband Internet access, empowers people to easily produce, manipulate and distribute large amounts of visual content.

Such a situation raises complex challenges in various multimedia domains (copyright protection, illegal distribution and management of massive databases, ...). Despite the particular applicative target, issues connected to medical images identification, authentication, indexation, retrieval, searching, navigation, organization and manipulation have to be always addressed.

Let's consider the case of medical images. Inside PACS (Picture Archiving and Communications system) environments deployed in hospitals, the medical images are protected from outside intruders by network firewalls. However, when exiting the protected network of the hospital and entering the public networks to the physician's and patient's home (for teleradiology and other telehealth applications), the medical images are no longer protected. Consequently, intruders, casual or with malicious intent, can tamper the image data, [MUL 04].

As an example, in Table 7: , a medical image can be altered/compromised during its transmission by a malicious user which can insert artifacts within an image and defy its detection. Table 7 is a digital mammogram with 2D artificial calcifications inserted [CAO 03]. Table 7(a) is the original mammogram, (b) the mammogram with artificial calcifications added, (c) the magnification of a region containing some added artifacts, and (d) is the subtracted images between the original and the modified mammogram. Calcifications are very small subtle objects within a mammogram. If inserted, artifacts would create confusion during diagnosis.



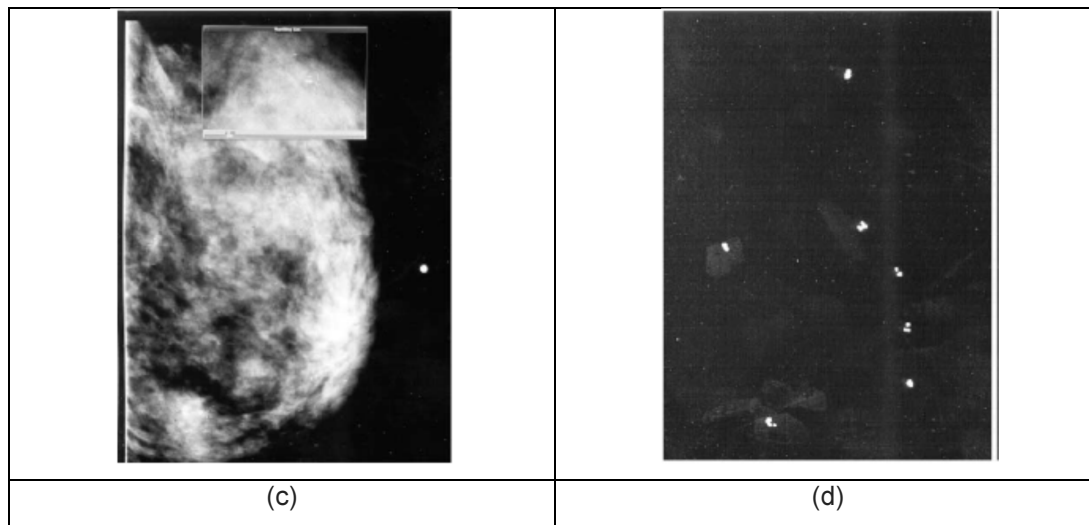


Table 7: A digital mammogram with inserted artificial calcifications: (a) original mammogram; (b) with artifacts; (c) magnification of some artifacts; (d) subtracted between (a) and (b). The artifacts are highlighted with overexposure during display [CAO 03]

To solve the issue of tracking and identifying replica images obtained by applying minor or major distortions on the original image, a solution intensively considered in research studies is image fingerprinting (also referred to as content-based copy detection or near-duplicate copy detection).

Throughout the current study, a copy, a replica or an attacked image is obtained from some original image content by means of any transformation/distortion, such as addition, deletion, modifications (of aspect, color, contrast, encoding, ...), or printing and scanning.

8.3.1.1 Definition

Image fingerprints can be best defined in relation with human fingerprints, [OOS 02], as illustrated in Figure 17. While the human fingerprint can be seen as a human summary (a signature) that is unique for every person, the image fingerprint can be seen as some short image feature (e.g. a string of bits, color histograms, ...) which can uniquely identify that image. In practice, image fingerprints are used just as human fingerprints: they are first computed and then searched for in a database, according to a given similarity measure.

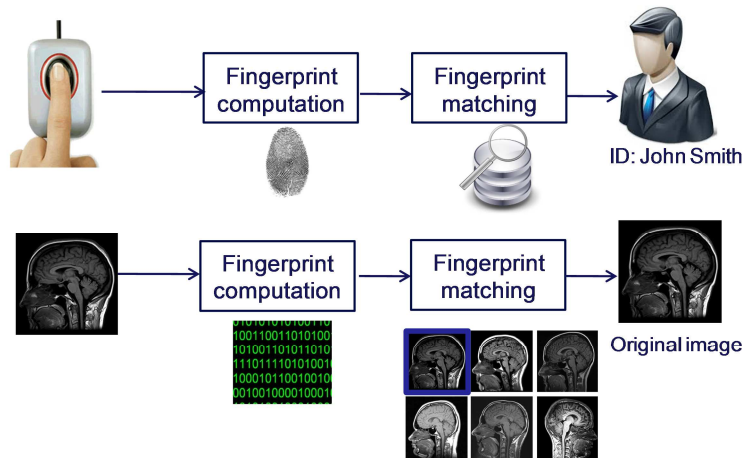


Figure 17: human fingerprinting and medical image fingerprinting

8.3.1.2 Properties

Assume the case in which an image has its fingerprints computed and is searched for in the database. A correct answer in such a matching procedure is obtained when the same visual content is detected not only in its original image but also in all its replica images; be there tp the number of such correct answers. A correct answer is also obtained when two images with different content are detected as different; be there tn , the number of such situations. Practical fingerprinting methods may also come across with two types of matching errors. First, some image content existing in the database might not be retrieved; be fn the number of such erred decisions. Secondly, the detection procedure can also yield a false positive i.e. take some visual content for another one. Be fp the number of such situations.

Image fingerprinting has two main properties:

- **Uniqueness:** fingerprints extracted from different content images should be different. This property is assessed by the probability of false alarm (P_{fa}) defined by the following formula:

$$P_{fa} = \frac{fp}{tp + fn + fp + tn}$$

- **Robustness to distortions:** fingerprints extracted from an original image and its replicas should be similar in the sense of the considered similarity metric. The robustness property is also quantified by the probability of missed detection (P_{md}), as defined below:

$$P_{md} = \frac{fn}{tp + fn + fp + tn}$$

On the one hand, an efficient fingerprinting method should ensure a low probability of false alarm (i.e. low probability of retrieving image which are neither the query nor its replicas) and low probability of missed detection (i.e. a low probability of not retrieving replica images of the query). According to the targeted application, additional functional properties, such as the database search efficiency can be set.

8.3.1.3 Use cases

8.3.1.3.1 Image identification and retrieval

Image identification and retrieval is at the heart of all systems dealing with images. The ability to identify and retrieve images even under distortions is a powerful tool for increasingly many applications.

Given a very large database of images and a query image, the identification of such a query can pose complex challenges (e.g. time requirements, human observers). An image fingerprinting system enables the identification of a particular image by computing its fingerprint and by efficiently querying it among the reference fingerprints without using human observers, Figure 18.

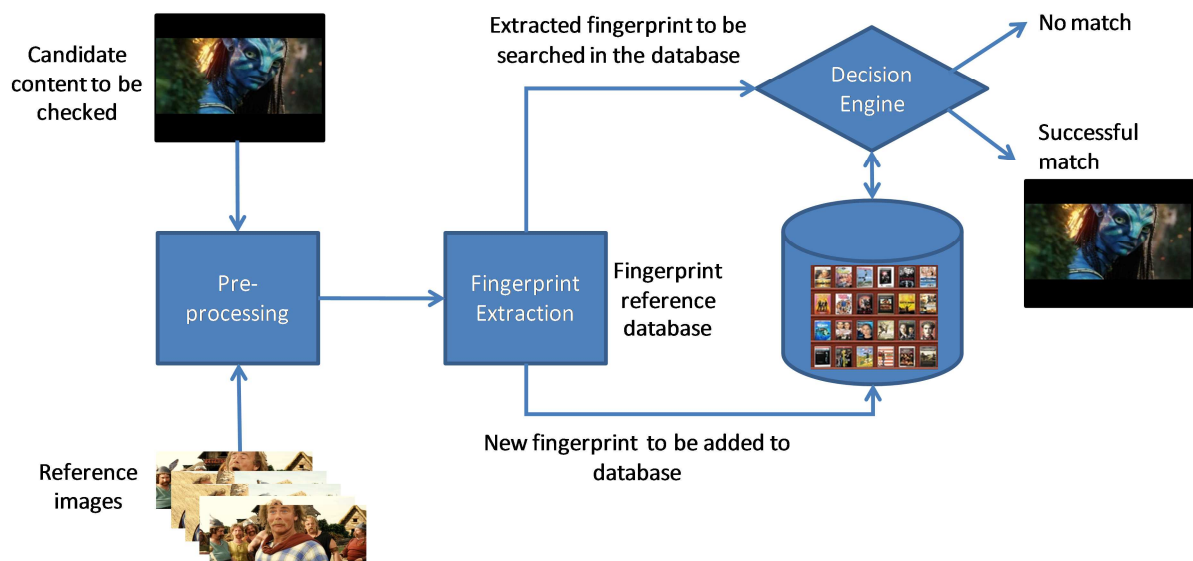


Figure 18: Image identification and retrieval

A possible use case for identification of multimedia in large databases is interactive advertising. In Figure 19, an agency has created a digital fingerprint for their specific TV commercial. When the fingerprint of the content playing on the screen is detected, a pop-up overlay dialog box is triggered on top of the advertisement asking the viewers if they want to take advantage of the coupon being offered on screen. By pressing their TV remote select button the viewers confirm they would like the coupon offered. Using the LAN connection, a coupon request is sent via the Internet to the retail web site. The requested coupon is sent by the retailer to the viewer's smart phone [AUD 12c].

The image fingerprinting scheme employed in the identification and retrieval of images from large databases has to be adapted to the use case.



Figure 19: interactive advertising

8.3.1.3.2 Authentication of multimedia content

Due to powerful software (e.g. Photoshop, Windows Movie Maker, Pinnacle) for multimedia manipulation, content became very easy to manipulate and alter (e.g. change of hair color of one of the characters), therefore in many cases the originality of the content might need to be checked. An authentication system based on fingerprinting verifies the originality of the content and aims at detecting the malicious transformation. This is achieved by designing a fingerprint and a similarity metric able to detect any minor transformation in the query compared to the original version.

8.3.1.3.3 Copyright infringement prevention

Web 2.0 services like Flickr, Instagram or Pinterest offer platforms for users to view and exchange images. Such websites need technology able to detect copyright infringement in their images database. Such technology relies on image fingerprinting principles. In order to achieve copyright infringement-free image database by means of image fingerprinting, content owners would have to provide reference fingerprints to user generated content sites, which would allow through the matching procedure the identification of the images. According to this identification and to the business or copyright rules established for each image, action can be taken, e.g. allow, filter, notify as illustrated in Figure 20.

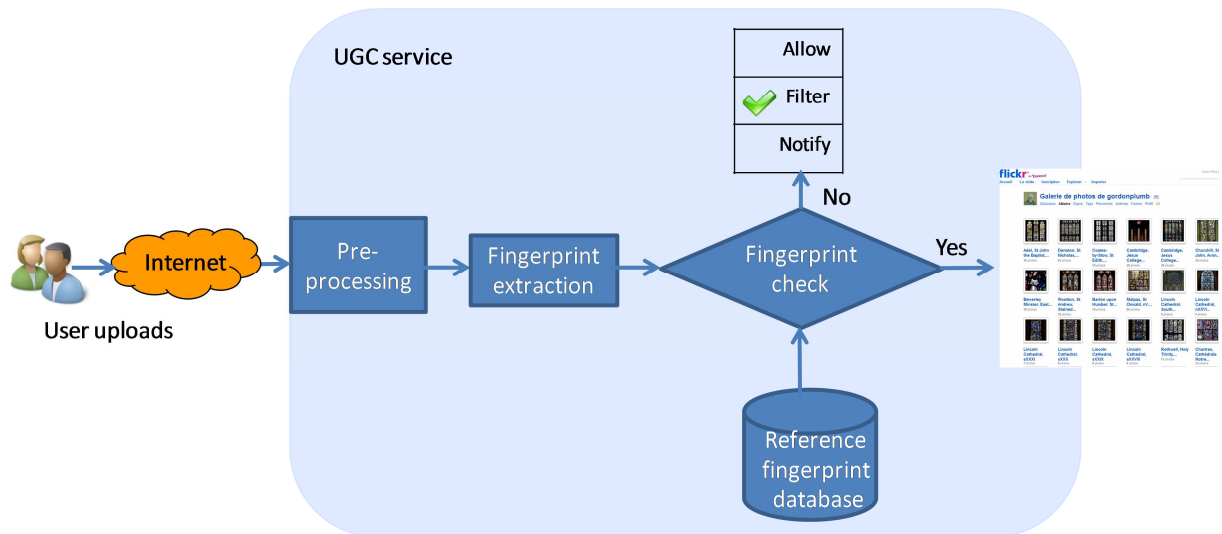


Figure 20: image filtering in UGC platforms

8.3.2 State of the art

The academic state of the art for image fingerprinting exhibits a large variety of methods addressing a large variety of applications and types of distortions.

In the sequel, a presentation of the potential distortions is discussed in §8.3.2.1 and a comprehensive overview of state of the art fingerprinting solutions is presented in §8.3.2.2.

8.3.2.1 Distortions

Distortions	Examples
Image aspect	<ul style="list-style-type: none"> ▪ color modifications: conversion to grayscale; conversion to sepia ▪ color filtering or corrections ▪ decrease of color depth
	<ul style="list-style-type: none"> ▪ photometric changes: brightness, contrast, saturation ▪ gamma correction ▪ histogram equalization
	<ul style="list-style-type: none"> ▪ filtering: linear (Gaussian, sharpening), non-linear (median filter)
	<ul style="list-style-type: none"> ▪ noise addition
Image content	<ul style="list-style-type: none"> ▪ <i>affine transformations</i> <ul style="list-style-type: none"> ▪ geometric modifications: <ul style="list-style-type: none"> ○ uniform or non-uniform scaling, rotations ○ reflection ○ aspect ratio changes ○ dilations

	<ul style="list-style-type: none"> ○ contractions ○ shear ▪ similarity transforms (spiral similarity) ▪ translations ▪ <i>cropping</i> <ul style="list-style-type: none"> ▪ letterbox removal ▪ row or columns removal ▪ <i>insertion</i>: text, caption, pattern, letter-box insertion ▪ <i>shifting</i> ▪ <i>StirMark</i>
Mixed	<ul style="list-style-type: none"> ▪ combinations of all the above modifications

Table 8: Types of image modifications: they can be induced in the content with computer software or by means of image printing, scanning, copying

8.3.2.1.1 Image aspect modifications

The modifications changing the aspect of the images refer to the following categories of distortions: color, photometric, filtering and noise addition.

The color modifications consist in changing the composition of the color balance in the images (i.e. modifying the values of the pixels' colors), changing the color depth (i.e. changing the numbers of bits used to represent the color of an image pixel: 1-bit color, monochrome; 8-bit color, 256 colors; 24-bit color true color more than 16 million colors; 30-48-bit color, deep color), converting the image in grayscale, filtering a certain color channel (R, G, B) or swapping colors (i.e. RGB to BGR, replacing the red color channel with the blue one, or other configurations).

Adjustments in the brightness (i.e. in the RGB color space, brightness is the arithmetic mean of the red, green and blue color coordinates), contrast (i.e. the difference between the black and white levels in images), saturation (i.e. the dominance of hue in the color), gamma corrections (i.e. a nonlinear operation $V_{out} = AV_{in}^\gamma$, where A is a constant and V is the value of a pixel, which changes the brightness of an image) or histogram equalizations (i.e. enhancement of the contrast of the images) of an image are the photometric distortions a image often subsists.

Image filtering is an operation which consists in removing some unwanted components of the 2D signal which is the image. The Gaussian filtering or blurring is a type of linear filtering which passes the low frequencies and attenuates the high frequencies, i.e. attenuating the contours of the shapes in the images. Sharpening is a type of linear filtering, which attenuates the low frequencies but passes the high frequencies, hence keeping the details in the images. Median filtering is a non-linear filtering operation used to remove noise from images and which is usually used in pre-processing steps in order to enhance the results of further processing, e.g. edge detection.

Image noise addition consists of adding a noise signal (Gaussian noise, white noise, salt and pepper noise) to the images in order to decrease its quality. The noise can be added by image processing operations or can be produced by the sensors and circuitry of digital cameras when taking a photo.

The color and photometric modifications as well as filtering and noise addition can be induced in images by image processing operations or intrinsically by taking a photo

with an external camera which implicitly change the colors and the values of the photometric parameters due to the device dependent sensors, circuitry and transducers' parameters.

8.3.2.1.2 Image content modifications

The distortions which modify the content of the image itself can be of the following types: affine transformations, cropping, insertion, picture in picture, rows or columns shifting. By changing the intrinsic content of the images, these modifications are difficult to handle by fingerprinting systems and generally require dedicated pre-processing blocks before the fingerprinting solution is deployed, e.g. letterbox removal block, detection and removal of caption, text or pattern, detection and extraction of the image of interest from the background or the foreground.

The affine transforms are the transforms which preserve the collinearity of points (i.e. all points lying on a line initially still lie on a line after the transformation) and ratios of distances (i.e. the midpoint of a line segment remains the midpoint after transformation).

The affine transformations for images include the following types of modifications: geometric contraction, expansion, dilation, reflection, rotation, shear, translations, and their combinations. In general, the affine transformations are a combination of rotations, translations, dilations and shears.

An example of affine transformation is the rotation-enlargement transformation which combines a rotation and an expansion and can be mathematically written as below:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = s \begin{bmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Where (x', y') are the coordinates of the rotated point, (x, y) are the coordinates of the original point, s is the scale factor and α is the rotation angle.

Such distortions are induced in images either by using image processing software e.g. the Adobe Photoshop or by means of taking a photo, printing the photo and then scanning it or copying it, Figure 21.

Scaling or resizing consists in changing the dimensions of the images, e.g. dilations or contractions of the height and width. Scaling can be done with the same scale factor for both height and width of images (i.e. uniform/isotropic scaling) with different scale factor i.e. non-uniform, anisotropic scaling. The advantage of using uniform scaling is the fact that it preserves the shapes of objects inside the images whereas non-uniform scaling changes these shapes. However in practice both scaling are intensively used in all types of applications, hence the modifications they induce in images have to be addressed by the image fingerprinting systems.



Original version	Camera replicas
------------------	-----------------

Figure 21: Affine transforms induced by camcording

Small rotations (with angles ranging from $\pm 1^\circ$ to $\pm 5^\circ$) often combined with cropping and scaling affect the image content itself by removing the cropped parts and therefore can make an image fingerprinting system to mistakenly take the rotated, cropped and resized content for a new content and not a replica. In Figure 22 an original image is trigonometrically rotated with 2° , 3° 5° and 10° in column (a) and cropped and resized in column (b). It can be noticed that up to 5° rotation the image content is visually similar to the original while the 10° rotation and cropping removes a large part of the initial content.


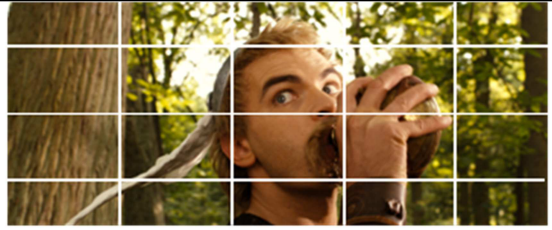

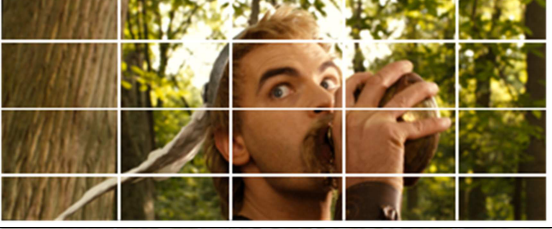

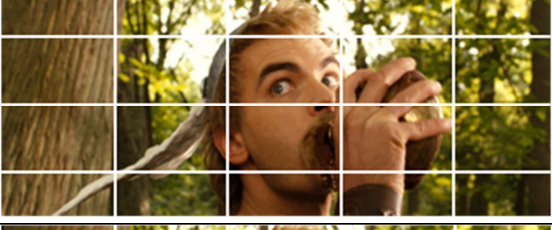

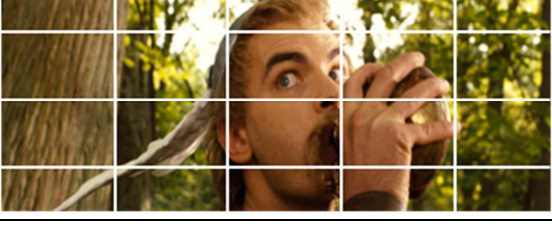
		Original images	
Rot deg		Rotated images	Rotated and cropped images
			
2°			
3°			
5°			



Figure 22: Images rotated with 2°, 3°, 5° and 10° in (a) column and images rotated and cropped in (b) column

Reflection or vertical flipping consists of generating a replica image by mirror-reversal of an original image as illustrated in Figure 23.



Figure 23: vertical flipping

Cropping consists in removing certain parts of the images content such as letter boxes, rows or columns depending on the application. Insertion of content does the reverse of cropping, which is inserting other visual content in the images such as text, captions, patterns, letter-boxes.

Picture in picture consists in displaying two images in the same time on a screen, one image being the foreground and one image being the background as illustrated in Figure 24.a.



Figure 24: television specific modifications

Cropping, insertion and picture in picture modifications are widely used in post-production and television processing of the images when several images are needed to be displayed at the same time on the screen or other information relevant for the broadcast program, news or other announcements are necessary, Figure 24.b.

Image shifting consists in moving to the right, to the left, up or down a certain amount of columns or rows of the images. The amounts of columns or rows shifted can vary between 1% to 5% of the image's width or height as it easily affects the visual quality of the image.

StirMark is a software package developed by Fabien Petitcolas [PET 00] which is generally used for benchmarking watermarking schemes. The software package contains several attacks such as cropping, rotation, rotation-scale, sharpening, Gaussian filtering, aspect ratio modifications and the StirMark random bending attack. The most well known is the StirMark random bending attack, or random geometric distortion which applies a combination of minor geometric distortions i.e. the image is slightly stretched, sheared, shifted and/or rotated by an unnoticeable random amount and finally re-sampled.

8.3.2.2 Image fingerprinting systems

Considering the two main blocks of a fingerprinting system, presented in Figure 17, namely the fingerprint computation and the fingerprint matching a classification can be made on two criteria: the type of features chosen as fingerprints and on the type of similarity metric employed between fingerprints.

8.3.2.2.1 Features

The first key component of an image fingerprinting system is the fingerprint. The quality of the fingerprint and its properties depend on the fingerprint features selected from the images. The types of features which were used in the state of the art as fingerprints are presented in Table 9.

The state of the art can be structured in four categories according to the domain in which the fingerprints are computed: spatial, transform, color and combined.

The spatial fingerprints computed on blocks, regions of images or whole images are robust to non-geometric distortions, but they lack in robustness against geometric modifications (e.g. cropping, rotations). The interest points based features have a high robustness against the geometric distortions but they are more sensitive to changes in color, illumination and filtering. Moreover, this type of features poses problems of uniqueness in the case of very similar images such as the medical images, therefore needs to be used in combination with other features.

Transform based fingerprints ensure robustness to geometric and non-geometric image aspect modifications but are sensitive to modifications of image content such as cropping and content addition.

The color based category of fingerprints lacks resilience to global variations in color and illumination but can be used along with other features in order to enhance discriminability.

The combined category of fingerprints generally provides the best results as they are able to address most of the transformations envisioned in image fingerprinting systems be them photometric or geometric.

Types of fingerprints	Fingerprint examples
-----------------------	----------------------

Spatial	<ul style="list-style-type: none"> ▪ visual attention regions of images, [SU 09] ▪ ordinal ranking of average gray level of image blocks, [HAM 02], [KIM 09] ▪ invariant moments of image edge representation, [HU 62] ▪ centroid of gradient orientations of images, [LEE 08] ▪ dominant edge orientation of images, [HAM 01] ▪ scale-space features (e.g. SIFT), [SAR 08] ▪ descriptors of interest points, [MAS 06]
2D Transform	<ul style="list-style-type: none"> ▪ quantized compact Fourier-Mellin transform coefficients of images, [SAR 08] ▪ subspace embedding using the singular value decomposition [RAD 08] ▪ the signs of DCT coefficients of images, [ARN 09] ▪ the averages of DC coefficients blocks of images, [YAN 08] ▪ DCT coefficients of the radial projection vector of the image pixels, [ROO 05] ▪ 2D wavelet transform, [GAR 11a], [GAR 11b], [GAR 12], [DUT 10]
Color	<ul style="list-style-type: none"> ▪ YUV histograms of the DC sequence of images [NAP 00], [HAM 07] ▪ YCbCr histogram of images, [SAR 08] ▪ color moment representation, [GAU 01] ▪ RGB, HSV histogram of images, [HAM 01] ▪ the principal component of the color histograms of images, [SAN 99]
Combined	<ul style="list-style-type: none"> ▪ SIFT, GIST and color correlogram features for images, [HIL 10] ▪ global visual feature (DCT), local visual feature (SIFT, SURF), [GAO 10] ▪ visual feature: center-symmetric local binary pattern (CS-LBP), hamming embedding; [JEG 10], [AYA 11] ▪ coarsely quantized area matching – visual feature, [FOU 11], [MUK 11] ▪ cascade of multimodal features (Dense Color SIFT, bag of words, DCT) and temporal pyramid matching, [JIA 11]

Table 9: types of image fingerprints

8.3.2.2.2 Similarity measures

The second key aspect of a fingerprinting system is the matching between the fingerprints. The matching can be achieved by employing a similarity metric adapted to the feature chosen as fingerprint and to the distortions envisioned.

According to the similarity distance employed for matching, the fingerprinting methods can be divided in two categories, distance based and probability based, as illustrated in Table 10.

Types of similarity measures	Similarity measure	Applicability
Distance based	L1 distance (Manhattan)	<ul style="list-style-type: none"> non-binary fingerprints, [HAM 01]
	L2 (Euclidian) distances	<ul style="list-style-type: none"> non-binary fingerprints, [LEE 08]
	Hamming distance	<ul style="list-style-type: none"> binary fingerprints [COS 06], [SU 09], [OOS 02]
	Hausdorff distance	<ul style="list-style-type: none"> edge points based fingerprints [HAM 01]
	Normalized histogram intersection	<ul style="list-style-type: none"> histogram based fingerprints [HAM 01]
	k-nn, voting function	<ul style="list-style-type: none"> interest point-based fingerprints, [LAW 06], [LAW 07], [JOL 07]
Probability based	Based on statistical tests	<ul style="list-style-type: none"> hypothesis testing, multivariate Wald-Wolforwitz, [DUT 10] Rho test on correlation, [GAR 11a], [GAR 11b]

Table 10: types of similarity measures for image fingerprinting

As it can be observed, a multitude of similarity measures are available, depending on the selected feature. The distance-based group of methods has the advantage of allowing a decision based on an experimentally determined threshold. While they are easier to use due to their immediate empiric observation, they don't permit in the majority of cases a decision based on a mathematical ground. Therefore the alternative is the probability-based similarity measures which can grant a statistical rule for decision.

The desideratum for a similarity measure under a fingerprinting framework is that it does not depend on an empirical threshold but on a rigorous mathematical decision rule which can handle any content, distortion or use case particularity.

8.3.3 Medical content based image retrieval

While image fingerprinting (i.e. content based copy detection) does not have a large deployment in the field of medical imaging, content based image retrieval (CBIR) exhibits a wide spread within numerous medical departments: dermatological images, cytological images, pathology images, tuberculosis smears, in cardiology for stenosis

images, radiology for mammographies, or classification of high resolution computer tomography. The CBIR systems can be used for the following applications:

- *teaching* – by browsing the large medical images repositories, various cases can be shown and analyzed together with the students. These cases can be chosen not only based on diagnosis or anatomical region but also visually similar cases with different diagnoses can be presented.
- *research* – by including visual features directly into medical studies, new correlations between the visual nature of a case and its diagnosis or textual description could be found. Visual data can also be mined to find changes or interesting patterns which can lead to the discovery of new knowledge.
- *diagnosis* - by supplying the medical doctor with cases that offer a similar visual appearance, clinical decision-making process can be enhanced. This can supply a second opinion for the medical doctor and (s)he can perform the reasoning based on the various cases that are supplied by the system and the data that is available on the current patient. Another idea is the creation of databases containing normal (non-pathologic) cases and compare the distance of a new case with the existing cases doing thus dissimilarity retrieval as opposed to similarity retrieval (distance to normality). A dissimilarity could be combined with highlighting regions in the image where the strongest dissimilarity occurred.

Following the approach used to present the image fingerprinting state of the art, a classification of the image CBIR systems is performed in the sequel. The systems are classified based on the features (§8.3.3.1) and on the similarity metrics (§8.3.3.2) used to obtain the image retrieval.

8.3.3.1 Features for image CBIR systems

Types of fingerprints	Papers
Color and grey level features	<ul style="list-style-type: none"> • histogram of color and grey level features [TAN 98], [KWA 02], [BRO 99] • local and global grey level features, [MUL 03] • statistical distribution of grey levels, [ANT 02], [ORP 96], [ELK 00], [QI 99], [BUE 002], [BUC 02], [LIU 00] • brightness histogram [QI 99]
Texture features	<ul style="list-style-type: none"> • Canny operator, [VER 98] • Sobel descriptors [BRO 99] • Fourier descriptors [ANT 02],[MAT 00], [BRO 99] • co-occurrence matrices features [BER 01], [ORH 96],[KWA 02], [BRO 99] • invariant moments features [ANT 02], [BUE 02], [MAT 00] • Gabor filters [TAN 98], [TAN 00],[MUL 03] • wavelets [VER 98],[KWA 02] • Markov texture characteristics [MAT 00] • denseness [BAE 02]

Shape of segments	<ul style="list-style-type: none"> • segmentation of pathologic images is described [WAN 00] • even shape descriptors for 3D structures using modal modeling, [SCL 94] • Fourier descriptors [COM 98], [LIU 132], [VER 98] • pattern spectrum [KOR 98] • morphological features [KOR 98] • signatures of the manually segmented objects, [ELK 00]
Local features	<ul style="list-style-type: none"> • bag of features, [WAN 96-11]
Eigenimages	<ul style="list-style-type: none"> • [SIN 02], [BUC 96]
Combined	<ul style="list-style-type: none"> • salient regions detected with wavelet pyramids and geodesic morphology, [FON 13]

Table 11: types of image features for CBIR use cases

8.3.3.2 Similarity metrics for image CBIR systems

Types of similarity measures	Similarity measure	References
Distance based	Euclidian vector space model (L1, L2)	<ul style="list-style-type: none"> ▪ majority of systems, [QI 99], [BUE 002], [BUC 02],
	principal component analysis	<ul style="list-style-type: none"> ▪ [SIN 02], [BUC 96]
	minimum description length	<ul style="list-style-type: none"> ▪ [BRO 99]
	kd-trees	<ul style="list-style-type: none"> ▪ [ROB 96]
	support vector machines	<ul style="list-style-type: none"> ▪ [QUD 12]
	R-trees	<ul style="list-style-type: none"> ▪ [PAT 97]
Statistically based	Bayesian networks	<ul style="list-style-type: none"> ▪ [LIU 97]
	neural networks	<ul style="list-style-type: none"> ▪ [HAN 96], [BAE 02]
	hidden Markov models	<ul style="list-style-type: none"> ▪ [BER 01]

Table 12: types of similarity measures for CBIR use cases

8.3.4 Conclusions

Fingerprinting consists in computing a signature for some visual content and in subsequently matching it (according to a similarity metric) to the reference database in order to track that content.

The fingerprinting main properties are uniqueness (fingerprints extracted from different content images should be different), robustness (fingerprints extracted from an original image and its replicas should be similar in the sense of the considered similarity metric) and database search efficiency (computation of the fingerprints and the matching procedure should ensure low, application dependent computation time for the image's retrieval).

While this concept is general, each applicative field (cinematography copyright protection, medical imaging security, database filtering) comes across with different practical constraints.

In the field of medical image fingerprinting for security purposes, the distortions that must be handled have a large variety: cropping, content addition, photometric distortions (contrast, brightness, saturation changes), geometric distortions (rotations, translations and combined affine transforms). All these distortions raise methodological and applicative challenges.

To our best knowledge, there is a large variety of content based image retrieval (CBIR) techniques, yet no medical image fingerprinting scheme. MEDUSA can be a first key player in developing such a technology by combining academic know-how on entertainment content fingerprinting with strong industrial expertise in security.

9 Present equipment and standard regulations

9.1 Introduction

This section provides common, high-level security and privacy standards for all healthcare products, services or service-related products. Compliance with these requirements provides appropriate protection of the confidentiality, integrity, and availability in Philips products, services or service-related products as deployed in our customers environment. This meets the following needs:

- customer SECURITY and privacy requirements, especially those imposed by national and regional regulatory frameworks such as the European Commission Directive 95/46 EC and the United States Health Insurance Portability and Accountability Act (HIPAA);
- protection of the CONFIDENTIALITY of information processed by Philips Healthcare PRODUCTS, SERVICES or SERVICE-RELATED PRODUCTS;
- enhancement of the INTEGRITY and AVAILABILITY of deployed Philips Healthcare PRODUCTS, SERVICES or SERVICE-RELATED PRODUCTS;
- protection of the Philips brand by ensuring that Philips Healthcare devices are not easily compromised and that ownership of privacy and SECURITY RISK is clear to both Philips and the customer; and
- a “One Philips” approach to PRODUCT SECURITY and privacy that permits ease of management and customer communication per “Sense and Simplicity

Where malicious activities result in physical or safety threats, the distinction between security and safety policies becomes difficult to discern. In general, where system design can help maintain the integrity of hardware operation, safety is the governing policy (e.g., verifying operation of cut-off switches). Where system design can help maintain the integrity of software code under malicious threat, security is the governing policy (e.g., virus detection). As always, safety is the first priority.

Those standards addresses controls essential to the maintenance of confidentiality and the protection from malicious intrusion that might lead to compromises in integrity and availability of the medical device, software, or data maintained by the product, service or service-related product (including sensitive data).

9.2 Applicable standards and policies for MEDUSA

9.2.1 Context of applicability of standards / policies

Medical devices which are deployed around the world need to conform to a wide set of security regulations. Applicability of regulations and policies depend on two main aspects: the geographic location, country and the institution using the device.

The geographic location, country defines the local laws which are applicable for the security aspects of the device. This legislation details which international standards and policies are applicable to a concrete Medusa instance. One important aspect to notice in legislation is that most laws refer to ‘good practice’, i.e. the system has to adhere to commonly accepted policies in the security area without always fully detailing which regulation are then in effect. As Medusa is a new type of cloud based

system, it is quite important to look next to applicable guidelines for cloud deployments.

Due to the complexity of the legislation and because it is quite hard to translate the legislation to direct effects on your system in most countries there are institutions which provide such a translation.

For example in the Netherlands there is an institution called 'Nictiz' which provides a translation between the Dutch legislation and their practical effects on the organization and devices used.

Also the institutions/hospitals themselves are playing a role; they have a need to satisfy local legislation and also to support a smooth cooperation between various devices. From the need to a smooth integration between various devices hospitals often mandate that the devices they use comply with specific standards and policies.

9.2.2 Selection criteria for applicable standards and policies

9.2.2.1 Context

The previous section defines the context which helps in selecting standards and policies for Medusa.

Foremost Medusa has to comply with local legislation. As Medusa is targeted at Europe the Medusa system has to comply with European guidelines on security and privacy. Most European countries have local legislation mandating specific European guidelines. So for Medusa it is important to adhere to the European guidelines for security and privacy.

Next is that to be able to be deployable throughout Europe the Medusa system also needs to adhere to country specific legislation.

One example of country specific legislation is the Dutch 'BSN' a citizen identification number used by specific organizations. In the Netherlands is it mandatory by law to use that identification number when exchanging information between institutions. As Medusa enables information exchange among others between Dutch hospitals the applicability of that specific law and the impact of that law on Medusa architecture and design has to be addressed. Note that as such a hospital using a device has to comply to this kind of legislation Medusa has to enable adherence in these cases.

Next institutions are interested in smooth cooperation of medical devices. In that area two standards are quite relevant, one is the DICOM standard and the other are the IHE profiles.

As the applicability and measure of conformance to these standards depends on the needs of the various institutions from Medusa point of view we need to ensure we can enable the institutions to adhere to these standards in their usage of Medusa. Also due to the nature of Medusa, being a new form of cooperation between existing institutions some of these standards cannot be fully applied.

Another important consideration is the 'good practice' concept. Various institutions outside of the legal scope of Medusa are known to provide good standards and certification for security and usage also to support a vision of a worldwide Medusa such standards and policies need to be considered.

9.2.2.2 Selected Criteria

The following is the list of selection criteria for applicable standards and policies:

1. Legislation applicable in countries where Medusa is to be deployed
2. European legislation and guidelines
3. International standards expected by institutions/hospitals
4. Standards and policies expected from current 'good practice'

9.2.2.3 Selected Legislation and Policies on security

The legislation and policies on security are twofold. One aspect is ensuring security and privacy the other aspect of is a seamless integration in a hospital environment.

The list below is a focus on the security aspect.

Note that applicability of the selected legislation and policies are depending on specific choices in the Medusa security architecture. Only European and country specific legislation is mandatory for Medusa deployments.

Ref.#	Document Title
[1]	DHHS/NIH Protecting Personal Health Information in Research
[3]	DICOM: Part 15: Security and System Management Profiles
[6]	DoD Directive 8500.1 Information Assurance (IA). October 24, 2002
[7]	NSA/NCSC Rainbow Series and Related Documents
[8]	NSA Security Configuration Guides
[9]	IASE Security Technical Implementation Guides (STIGS) and Supporting Documents.
[10]	NIST Computer Security Division: DISA security technical implementation guides (stigs) and checklists
[12]	FDA Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-shelf (OTS) Software
[13]	European Directive EU 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[14]	HIPAA Advisory
[15]	HIPAA Privacy Rule: Standards for Privacy of Individually Identifiable Health Information.
[16]	HIPAA Security Rule: Standards for the Protection of Electronic Protected Health Information.
[17]	IHITSP/TN900 – Security and Privacy Technical Note, Version 1.2, August 2008
[18]	HITSP/C44 – Secure Web Connection Component, Version 2.2, August 2008,
[19]	HITSP/T17 – Secured Communication Channel Transaction, Version 1.2, August 2008
[20]	HITSP/T24 – Pseudonymize Transaction
[21]	IETF RFC-3881 Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications
[22]	IHE IT Infrastructure Technical Framework Volume 1 (ITI TF-1) Integration Profiles Revision 4.0
[23]	IHE ITI TF-1: 4: Enterprise User Authentication (EUA) profile (defined in [32])
[24]	IHE ITI TF-1: 9: Audit Trail and Node Authentication (ATNA) profile (defined in [32])

Ref.#	Document Title
[25]	IHE Technical Framework Volume III Transactions (continued) Revision 8.0 – Final Text August 30, 2007
[26]	IHE TF-III: 5.1: RAD TF (Radiology Audit Trail) (in [35])
[28]	NEMA SPC Security and Privacy Auditing in Health Care Information Technology. November 2001
[27]	NEMA SPC Security and Privacy: An Introduction to HIPAA. February 2001
[29]	NEMA SPC Break-Glass - An Approach to Granting Emergency Access to Healthcare Systems. December 2004
[30]	NEMA SPC Defending Medical Information Systems Against Malicious Software. December 2003.
[31]	NEMA SPC Patching Off-The-Shelf Software Used in Medical Information Systems. October 2004.
[32]	NEMA SPC REMOTE SERVICE INTERFACE - Solution (A): IPsec over the Internet Using Digital Certificates – Version 2. December 2003
[33]	NEMA SPC Management of Machine Authentication Certificates. May 2007
[34]	NEMA SPC Information Security Risk Management for Healthcare Systems. October 2007
[35]	NEMA Remote Services in Healthcare – Use Cases and Obligations For Customer and Service Organizations, September 2008
[36]	NEMA SPC Security and Privacy Auditing in Healthcare Information Technology, November 2001
[37]	NIST SP 800-66-Rev1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Oct 2008
[39]	NIST SP 800–14: Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996
[40]	NIST SP 800–33: Underlying Technical Models for Information Technology Security. December 2001
[41]	NIST SP 800-40v2: Creating a Patch and Vulnerability Management Program. November 2005.
[42]	NIST SP 800-63v1.0.2: Electronic Authentication Guideline. April 2006
[44]	NIST SP 800-70 National Checklist Program for IT Products--Guidelines for Checklist Users and Developers,
[45]	NIST SP 800-73-2: DRAFT Interfaces for Personal Identity Verification (4 parts). March 2008 - 1 - End-Point PIV Card Application Namespace, Data Model and Representation
[46]	NIST SP 800-73-2: DRAFT Interfaces for Personal Identity Verification (4 parts). March 2008 - 2 - End-Point PIV Card Application Interface.
[47]	NIST SP 800-73-2: DRAFT Interfaces for Personal Identity Verification (4 parts). March 2008 - 3 - End-Point PIV Client Application Programming Interface.
[48]	NIST SP 800-73-2: DRAFT Interfaces for Personal Identity Verification (4 parts). March 2008 - 4 – The PIV Transitional Data Model and Interfaces.
[49]	NIST FIPS 140-2 Security Requirements for Cryptographic Modules
[51]	NSA Security Configuration Guides.
[52]	ITU-T RECOMMENDATION X.509
[53]	OIS Guidelines for Security Vulnerability Reporting and Response – Organization for Internet Safety - V2.0. September 2004

9.2.2.4 Selected Legislation and Policies on system integration (for security aspects)

The legislation and policies on security are twofold. One aspect is ensuring security and privacy the other aspect of is a seamless integration in a hospital environment.

The list below is a focus on the integration aspect.

Note that applicability of the selected legislation and policies are depending on specific choices in the Medusa security architecture. The required choices also depend on needs of the involved hospitals/institutions.

Ref. #	Document title
[1]	DHHS/NIH Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule
[2]	DICOM STANDARD, Version 2008
[3]	DICOM: Part 15: Security and System Management Profiles
[4]	DICOM: Supplement 55: Attribute level confidentiality (including De-identification) 5 Sept 2002
[5]	DICOM Supplement 51: Media security 10 Sept 2001
[11]	GMP reference, CAPA
[15]	HIPAA Privacy Rule: Standards for Privacy of Individually Identifiable Health Information.
[16]	HIPAA Security Rule: Standards for the Protection of Electronic Protected Health Information. The
[17]	IHITSP/TN900 – Security and Privacy Technical Note, Version 1.2, August 2008,
[18]	HITSP/C44 – Secure Web Connection Component, Version 2.2, August 2008,
[19]	HITSP/T17 – Secured Communication Channel Transaction, Version 1.2, August 2008,
[21]	IETF RFC-3881 Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications
[22]	IHE IT Infrastructure Technical Framework Volume 1 (ITI TF-1) Integration Profiles Revision 4.0 - Final Text August 22, 2007 http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_4_0_Vol1_FT.pdf
[23]	IHE ITI TF-1: 4: Enterprise User Authentication (EUA) profile (defined in [32])
[24]	IHE ITI TF-1: 9: Audit Trail and Node Authentication (ATNA) profile (defined in [32])
[25]	IHE Technical Framework Volume III Transactions (continued) Revision 8.0 – Final Text August 30,
[26]	IHE TF-III: 5.1: RAD TF (Radiology Audit Trail) (in [35])
[29]	NEMA SPC Break-Glass - An Approach to Granting Emergency Access to Healthcare Systems.
[32]	NEMA SPC REMOTE SERVICE INTERFACE - Solution (A): IPsec over the Internet Using Digital
[33]	NEMA SPC Management of Machine Authentication Certificates. May 2007
[35]	NEMA Remote Services in Healthcare – Use Cases and Obligations For Customer and Service Organizations, September 2008
[36]	NEMA SPC Security and Privacy Auditing in Healthcare Information Technology, November 2001

Ref.#	Document title
[39]	NIST SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996

9.2.2.5 Critical legislation and guidelines based on the criteria (must do list)

Based on the defined criteria and focusing on legislation we need to select the following set.

Ref.#	Document title
[13]	European Directive EU 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
[22]	IHE IT Infrastructure Technical Framework Volume 1 (ITI TF-1) Integration Profiles Revision 4.0 - Final Text August 22, 2007
[37]	NIST SP 800-66-Rev1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Oct 2008

One important item to consider and requires further discussion with clinical partners in Medusa context is the following:

Ref.#	Document title
[29]	NEMA SPC <i>Break-Glass - An Approach to Granting Emergency Access to Healthcare Systems</i> . December 2004

10 Trusted execution on cloud nodes

This final section presents the main challenges for the Medusa system, regarding this state of the art on secure & dependable data transfer, and the architecture model.

10.1 Reference Model

It is critical to recognize that security is a cross-cutting aspect of the architecture that spans across all layers of the reference model, ranging from physical security to application security. Therefore, security in cloud computing architecture concerns is not solely under the purview of the Cloud Providers, but also Cloud Consumers and other relevant actors. Cloud-based systems still need to address security requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, audit, security monitoring, incident response, and security policy management. While these security requirements are not new, we discuss cloud specific perspectives to help discuss, analyze and implement security in a cloud system.

10.1.1 Cloud Service Model Perspectives

The three service models for cloud, i.e. SaaS, PaaS, and IaaS, present consumers with different types of service management operations and expose different entry points into cloud systems, which in turn also create different attacking surfaces for adversaries. Hence, it is important to consider the impact of cloud service models and their different issues in security design and implementation. For example, SaaS provides users with accessibility of cloud offerings using a network connection, normally over the Internet and through a Web browser. There has been an emphasis on Web browser security in SaaS cloud system security considerations. Cloud Consumers of IaaS are provided with virtual machines (VMs) that are executed on hypervisors on the hosts, therefore, hypervisor security for achieving VM isolation has been studied extensively for IaaS Cloud Providers that use virtualization technologies.

10.1.2 Implications of Cloud Deployment Models

The variations of cloud deployment models have important security implications as well. One way to look at the security implications from the deployment model perspective is the differing level of exclusivity of tenants in a deployment model. A private cloud is dedicated to one consumer organization, whereas a public cloud could have unpredictable tenants co-existing with each other, therefore, workload isolation is less of a security concern in a private cloud than in a public cloud. Another way to analyze the security impact of cloud deployment models is to use the concept of access boundaries. For example, an on-site private cloud may or may not need additional boundary controllers at the cloud boundary when the private cloud is hosted on-site within the Cloud Consumer organization's network boundary, whereas an out-sourced private cloud tends to require the establishment of such perimeter protection at the boundary of the cloud.

10.1.3 Shared Security Responsibilities

Cloud Provider and Cloud Consumer have different degrees of control over the computing resources. Compared to traditional IT systems, where one organization has

control over the whole stack of computing resources and the entire life-cycle of the systems, Cloud Providers and Cloud Consumers collaboratively design, build, deploy, and operate cloud-based systems. The split of control means both parties now share the responsibilities in providing adequate protections to the cloud-based systems. Security is a shared responsibility. Security controls, i.e., measures used to provide protections, need to be analyzed to determine which party is in a better position to implement. This analysis needs to include considerations from a service model perspective, where different service models imply different degrees of control between Cloud Providers and Cloud Consumers. For example, account management controls for initial system privileged users in IaaS scenarios are typically performed by the IaaS Provider whereas application user account management for the application deployed in an IaaS environment is typically not the provider's responsibility.

10.1.4 Medusa reference security architecture

Security is one of the most important categories of Medusa capabilities, given that data and user accounts are typically hosted by the SaaS provider. Medusa SaaS should provide the following capabilities:

- **Identity and federation.** Identity uniquely identifies a user or another entity such as an Intel application or system. An example is a user name. Federation describes the function of enabling users in one domain to securely and seamlessly access data within another domain.
- **Authentication and single sign-on (SSO).** The process of identifying an individual, usually based on a user name and password. In the context of SaaS, this includes the ability to achieve SSO across multiple cloud applications and services.
- **Authorization and role-based access control.** After an identity has been confirmed, authorization is the process of giving individuals access to system objects based on their identities. Identities are usually assigned to roles for ease of managing access.
- **Entitlement.** The process of granting access to a specific resource. Tenants are usually responsible for maintaining their own user accounts using delegated administration.
- **Encryption.** Data may need to be encrypted in transit (between applications or between the layers within an application) and at rest (while stored).
- **Regulatory controls.** Tracking and reporting who accessed what, when, and why. It includes tracking access to application features and data, the security rating of the data, and the implementation of a data retention policy. It also includes identifying whether individuals are located in controlled countries.

10.2 Secure Cloud Solutions

The work to be performed in WP4 of Medusa must provide to the precise Security needs of the global Architecture of the platform. With the introduction of Cloud Deployment technology two distinct security planes can be identified. On the one hand, the medical application domain, which, without the adjunction of cloud provisioning, would require stringent security measures in order to ensure the control of integrity and access to the personal medical data that will be processing in accordance with national and international medical legal requirements. On the other

hand, the application deployment plane, responsible for the deployment and configuration of the application components required for a particular use case instance of the medical application. These two security planes must be kept distinct in order to ensure both the administrative and medical integrity of the solution.

In addition to the currently recognised needs for Security for the protection of content and eventual transmission of the representational data subsequent security measures are to be put in place “from the ground up”, so to speak.

This requires that:

- All operational software components, in both the application and deployment planes, must be deployed on tamperproof platforms where attestation of trust can be constantly procured and verified in order to provide absolute assurance of the integrity of the underlying hardware, hypervisor and operating systems.
- All operational software components must cooperate in conjunction with the “single sign on” (SSO) procedure of their security plane and respect the associated requirements of the corresponding Authentication, Authorization and Accountability (AAA) procedures of the same plane.
- All operational software components will be controlled by and compliant with the centralised Organisational and Role based Access Control (ORBAC) Policy management system of the particular security domain.

The selection of particular technological solutions for the satisfaction of these three requirements of the two security planes is of fundamental importance for the assurance of the operational integrity of the resulting medical cloud system and the applications that it delivers.

10.3 Security in CompatibleOne ACCORDS platform

CompatibleOne offers a simple and unique interface allowing for the description of user cloud computing needs, in terms of resources, and their subsequent provisioning on the most appropriate cloud provider.

The security of the platform is based on the principles of Transport Layer Security and is compliant with the most recent specifications published by the IETF in this respect. The exchange of certificates between components of the platform is intended and strongly encouraged but not mandatory. The authorization and authentication of all communicating endpoints is required to be performed prior to any other activity when platform security has been activated.

The principles, on which the security of the platform depends, require the use of Transport Layer Security (TLS 1.0) to be announced and accepted by all server and client endpoints.

Currently the COSS (CompatibleOne Security Service) component itself plays the role of identity management but this role will be assumed by extensions or connectors to third party identity management packages of single sign on solutions.

The Authentication and Authorization layer enforces the required level of security as described by the security configuration parameters and involves:

- The configuration of the keys and certificates required by the Transport Layer Security

- The authentication of the user credentials provided by the application environment through the CompatibleOne Security Service working in conjunction with the identity management services.

Failure to comply with any of the security requirements will result in premature termination of accords services.

The lowest layer of the Acords interface architecture allows fine control over the Transport Layer Security (TLS) mechanisms and is responsible for the presentation and validation of PCKS certificates used for the ultimate identification of communicating end points.

Accords platform security can be enforced by the use of HSM, allowing the generation of RSA key pairs and X509 certificates by the HSM, which provides at the same time a hardware-based protection for private keys.

Bull has developed an OpenSSL engine which allows OpenSSL applications to use through a PKCS#11 interface the security functions provided by HSM, taking advantage of key storage in secure memory and acceleration of RSA and random functions.

Appendix 1: Fingerprinting & Watermarking references

- [ANT 02] S. Antani, L.R. Long, G.R. Thoma, A biomedical information system for combined content-based retrieval of spine X-ray images and associated text information, in: Proceedings of the Third Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2002), Ahamdabad, India, 2002.
- [BAE 02] S. Baeg, N. Kehtarnavaz, Classification of breast mass abnormalities using denseness and architectural distorsion, *Electronic Lett. Comput. Vis. Image Anal.* 1 (1) (2002) 1—20.
- [BER 01] S. Beretti, A. Del Bimbo, P. Pala, content-based retrieval of 3D cellular structures, in: Proceedings of the Second International Conference on Multimedia and Exposition (ICME'2001), IEEE Computer Society, IEEE Computer Society, Tokyo, Japan, 2001, pp. 1096—1099.
- [BRO 99] C. Brodley, A. Kak, C. Shyu, J. Dy, L. Broderick, A.M. Aisen, Content-based retrieval from medical image databases: A synergy of human interaction, machine learning and computer vision, in: Proceedings of the 10th National Conference on Artificial Intelligence, Orlando, FL, USA, 1999, pp. 760—767
- [BUC 96] G. Bucci, S. Cagnoni, R. De Domicinis, Integrating content-based retrieval in a medical image reference database, *Comput. Med. Imag. Graphics* 20 (4) (1996), 231—241.
- [BUE 02] J.M. Bueno, F. Chino, A.J.M. Traina, C.J. Traina, P.M. Azevedo-Marques, How to add content-based image retrieval capacity into a PACS, in: Proceedings of the IEEE Symposium on Computer-Based Medical Systems (CBMS 2002), Maribor, Slovenia, 2002, pp. 321—326.
- [CAO 03] Cao, F., Huang, H. K., & Zhou, X. Q. (2003). Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics*, 27(2), 185-196.
- [COM 98] D. Comaniciu, P. Meer, D. Foran, A. Medl, Bimodal system for interactive indexing and 18 retrieval of pathology images, in: Proceedings of the Fourth IEEE Workshop on Applications of Computer Vision (WACV'98), Princeton, NJ, USA, 1998, pp. 76—81.
- [DUT 10] Dutta, D, Saha, S.K., Chanda, B., “A hypothesis test based robust technique for video sequence matching,” *International Journal of Future Generation Communication and Networking*, Vol. 3, No.3, 2010.
- [ELK 00] E. El-Kwae, H. Xu, M.R. Kabuka, Content-based retrieval in picture archiving and communication systems, *J. Digital Imag.* 13 (2) (2000) 70—81.
- [FON 13] Foncubierta-Rodriguez, A., Müller, H., & Depeursinge, A. (2013, March). Region-based volumetric medical image retrieval. In *SPIE Medical Imaging* (pp. 867406-867406). International Society for Optics and Photonics.

- [FOU 11] Foucher, S., Lalonde, M. Gupta, V., Darvish, P., Gagnon L., Boulianne, G., "CRIM Notebook Paper - TRECVID 2011 Surveillance Event Detection", *Proceedings of TRECVID 2011*.
- [GAO 10] Gao, W., Huang, T., Tian, Y., Wang Y., Li, Y., Mou, L., Su, C., Jiang, M., Fang, X., Qian, M., "PKU-IDM@TRECVID-CCD 2010: Copy Detection with Visual-Audio Feature Fusion and Sequential Pyramid Matching", *Proceedings of TRECVID 2010*.
- [GAR 11a] Garboan, A., Mitrea, M., Prêteux, F., "DWT-based Robust Video Fingerprinting", *Proceedings for the "3rd European Workshop on Visual Information Processing" (EUVIP), 2011, Paris, pp. 216 - 221*.
- [GAR 11b] Garboan, A., Mitrea, M., Prêteux, F., "Video retrieval by means of robust fingerprinting", *Proceedings for the "15th IEEE Symposium on Consumer Electronics" (ISCE), 2011, Singapore, pp. 299 - 303*.
- [GAU 04] Gauch, J. M., "Real-time feature-based video stream validation and distortion analysis system using color moments", United States Patent 6246803.
- [GIO 99] Gionis, A., Indyk, P., Motwani, R., "Similarity Search in High Dimensions via Hashing", *Proc. 25th VLBD Conference Edinburgh, Scotland 1999*
- [HAM 01] Hampapur, A., Bolle, R.M., "Comparison of distance measures for video copy detection", IBM TJ Watson Research Center, *IEEE International Conference on Multimedia and Expo, 2001, pp. 737 - 740*.
- [HAM 02] Hampapur, A., Hyun, K-H., Bolle, R., "Comparison of Sequence Matching Techniques for video copy detection", in *Proceedings of Storage and Retrieval for Media Databases (San Jose, USA, Jan. 20-25, 2002)*, pp: 194-201.
- [HAN 96] R. Hanka, T.P. Harte, Curse of dimensionality: classifying large multi-dimensional images with neural networks, in: *Proceedings of the European Workshop on Computer-Intensive Methods in Control and Signal Processing (CIMCSP 1996)*, Prague, Czech Republic, 1996.
- [HIL 10] Hill, M., Hua, G., Natsev, A., Smith, J.R., Xie, L., Huang, B., Merler M., Ouyang, H., Zhou M., "IBM Research TRECVID-2010 Video Copy Detection and Multimedia Event Detection System", *Proceedings of TRECVID 2010*.
- [HUA 04] Hua, X.-S., Chen, X., Zhang, H.-J., 2004. "Robust video signature based on ordinal measure", in: *Proceedings of the IEEE International Conference on Image Processing (ICIP), 2004, Vol. 1, 24-27, 2004, pp. 685-688*.
- [HU 62] Hu, M.K., "Visual pattern recognition by moment invariants", *Transactions on Information Theory*, Vol. IT-8, pp: 179-187, 1962.
- [IND 99] Indyk, P., Iyengar, G., Shivakumar, N., "Finding Pirated Video Sequences on the Internet", Stanford Infolab, 1999.
- [JEG 10] Jégou, H., Gros, P., Douze, M., Schmid, C., Gravier, G., "INRIA LEAR-TEXMEX: Video Copy Detection Task", *Proceedings of TRECVID 2010*
- [JIA 11] Jiang, M., Shu, F., Tian, Y., Huang, T., "Cascade of Multimodal Features and Temporal Pyramid Matching", *Proceedings of TRECVID 2011*.
- [JOL 05] Joly, A., Frélicot, C., Buisson, O., "Content-based video copy detection in large databases: A local fingerprints statistical similarity search approach", in *Proceedings of the International Conference on Image Processing, 2005*.

- [KIM 05] Kim, C., Vasudev, B., "Spatio-temporal sequence matching for efficient video copy detection", in *Proceedings of the IEEE Transactions on Circuit Systems Video Technology*, 15 (1), 2005, pp.127–132.
- [KIM 09] Kim, J., Nam J., "Content-based video copy detection using spatio-temporal compact feature", *Proceedings of the 11th international conference on Advanced Communication Technology (ICACT)*, Vol. 3, 2009.
- [KOR 98] P. Korn, N. Sidiropoulos, C. Faloutsos, E. Siegel, Z. Protopapas, Fast and effective retrieval of medical tumor shapes, *IEEE Trans. Knowledge Data Eng.* 10 (6) (1998) 889–904.
- [KOCH 85] Koch, C., Ullman, S., "Shifts in selective visual attention: towards the underlying neural circuitry", *Human neurobiology*, Vol. 4, No. 4. (1985), pp: 219-227, 1985.
- [KWA 02] D.-M. Kwak, B.-S. Kim, O.-K. Yoon, C.-H. Park, J.-U. Won, K.-H. Park, Content-based ultrasound image retrieval using a coarse to fine approach, *Annals New York Acad. Sci.* 980 (2002) 212—224.
- [LAW 06] Law-To J., Buisson O., Gouet-Brunet, Boujemaa N., "Robust voting algorithm based on labels of behavior for video copy detection", *14th ACM International Conference on Multimedia*, pp.835 – 844, Santa Barbara, USA, 2006.
- [LAW 07] Law-To, J., Buisson, O., Gouet-Brunet, Boujemaa, N., "Video copy detection on the Internet": The challenges of copyright and multiplicity", *IEEE International Conference on Multimedia & Expo*, pp. 2082 - 2085, Beijing, 2007.
- [LAZ 06] Lazebnik, S., Schmid, C., Ponce, J., "Beyond Bags of Features: Spatial Pyramid Matching for Recognizing Natural Scene Categories", *CVPR'06*, Vol. 2, pp. 2169-2178, June 17-22, 2006.
- [LEE 08] Lee, S., Yoo C.D., "Robust video fingerprinting for content-based video identification", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 18, No. 7, 2008.
- [LIU 01] C.-T. Liu, P.-L. Tai, A.Y.-J. Chen, C.-H. Peng, T. Lee, J.-S. Wang, A content-based CT lung retrieval system for assisting differential diagnosis images collection, in: *Proceedings of the second International Conference on Multimedia and Exposition (ICME'2001)*, IEEE Computer Society, IEEE Computer Society, Tokyo, Japan, 2001, pp. 241—244.
- [LIU 97] Y. Liu, F. Dellaert, Classification-driven medical image retrieval, in: *Proceedings of the ARPA Image Understanding Workshop*, 1997.
- [LOW 04] Lowe, D. G., "Distinctive Image Features from Scale-Invariant Keypoints", *IJCV*, Vol. 60, No. 2, pp. 91-110, 2004.
- [MAS 06] Massoudi, A., Lefebvre, F., Demarty, C.H., Oisel L., Chupeau, B., "A Video Fingerprint Based on Visual Digest and Local Fingerprints", *IEEE International Conference on Image Processing*, Issue 8-11, pp. 2297 – 2300, 2006
- [MAT 00] M.E. Mattie, L. Staib, E. Stratmann, H.D. Tagare, J. Duncan, P.L. Miller, PathMaster: Content-based cell image retrieval using automated feature extraction, *J. Am. Med Informatics Assoc.* 7 (2000) 404—415.

- [MUL 04] Müller, H., Michoux, N., Bandon, D., & Geissbuhler, A. (2004). A review of content-based image retrieval systems in medical applications—clinical benefits and future directions. *International journal of medical informatics*, 73(1), 1-23.
- [MUL 03] H. Müller, A. Rosset, J.-P. Vallée, A. Geissbuhler, Integrating content-based visual access methods into a medical case database, in: *Proceedings of the Medical Informatics Europe Conference (MIE 2003)*, St. Malo, France, 2003,
- [OOS 02] Oostveen, J., Kalker, T., Haitsma, J., "Feature Extraction and a Database Strategy for Video Fingerprinting", *Lecture Notes In Computer Science*, Vol. 2314 archive, *Proceedings of the 5th International Conference on Recent Advances in Visual Information Systems*, pp. 117 – 128, 2002.
- [ORH 96] S.C. Orphanoudakis, C.E. Chronaki, D. Vamvaka, I2Cnet: content-based similarity search in geographically distributed repositories of medical images, *Comput. Med. Imag. Graphics* 20 (4) (1996) 193—207.
- [PAT 97] E.G.M. Patrakis, C. Faloutsos, Similarity searching in medical image databases, *IEEE Trans. Knowledge Data Eng.* 9 (3) (1997) 435—447.
- [QI 99] H. Qi, W.E. Snyder, Content-based image retrieval in PACS, *J. Digital Imag.* 12 (2) (1999) 81—83.
- [QUD 12] Quddus, A., & Basir, O. (2012). Semantic Image Retrieval in Magnetic Resonance Brain Volumes. *Information Technology in Biomedicine*, *IEEE Transactions on*, 16(3), 348-355.
- [RAD 08] Radhakrishnan, R., Bauer, C., "Robust Video Fingerprints Based on Subspace Embedding", *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2008, Las Vegas, pp. 2245 – 2248.
- [ROO 05] Roover, C. De, Vleeschouwer, C. De, Lefebvre, F., Macq B., "Robust video hashing based on radial projections of key frames", *IEEE Transactions on Signal Processing*, Vol 53, Issue: 10, pp. 4020 - 4030, 2005.
- [ROB 96] G.P. Robinson, H.D. Targare, J.S. Duncan, C.C. Jaffe, Medical image collection indexing: shape-based retrieval using KD-trees, *Comput. Vis. Graphics Image Proces.* 20 (4) (1996) 209—217.
- [SAN 99] Sánchez, J. M., Binefa, X., Vitrià, J., Radeva, P., "Local Color Analysis for Scene Break Detection Applied to TV Commercials Recognition", *Proceedings of the Third International Conference on Visual Information and Information*, pp: 237 – 244, 1999.
- [SAR 08] Sarkar, A., Ghosh, P., Moxley, E., Manjunath, B. S., "Video Fingerprinting: Features for Duplicate and Similar Video Detection and Query-based Video Retrieval", *Proceedings of SPIE - Multimedia Content Access: Algorithms and Systems II*, 2008.
- [SCL 94] S. Sclaroff, A.P. Pentland, On modal modeling for medical images: Underconstrained shape description and data compression, in: *Proceedings of the IEEE Workshop on Biomedical Image Analysis (BIA'1994)*, Seattle, WA, USA, 1994, pp. 70—79.
- [SEO 03] Jin S. Seo, Jaap Haitsma, Ton Kalker, Chang D. Yoo, "A robust image fingerprinting system using the Radon transform"
- [SIN 02] U. Sinha, H. Kangaroo, Principal component analysis for content-based image retrieval, *RadioGraphics* 22 (5) (2002) 1271—1289

[SU 09] Su, X., Huang, T., Gao, W., “Robust video fingerprinting based on visual attention regions”, in Proceedings of the International Conference on Acoustics, Speech and Signal Processing, 2009.

[TAN 98] L.H. Tang, R. Hanka, R. Lan, H.H.S. Ip, Automatic semantic labelling of medical images for content-based retrieval, in: Proceedings of the International Conference on Artificial Intelligence, Expert Systems and Applications (EXPERTSYS 1998), Virginia Beach, VA, USA, 1998, pp. 77—82.

[TAN 00] L.H. Tang, R. Hanka, H.H.S. Ip, R. Lam, Extraction of semantic features of histological images for content-based retrieval of images, in: Proceedings of the IEEE Symposium on Computer-Based Medical Systems (CBMS 2000), Houston, TX, USA, 2000.

[VER 98] K. Veropoulos, C. Campbell, G. Learnmonth, Image processing and neural computing used in the diagnosis of tuberculosis, in: Proceedings of the Colloquium on Intelligent Methods in Healthcare and Medical Applications (IMHMA), York, UK, 1998.

[WAN 96-11] Wang, J., Li, Y., Zhang, Y., Wang, C., Xie, H., Chen, G., & Gao, X. (2011). Bag-of-features based medical image retrieval via multiple assignment and visual words weighting. IEEE transactions on medical imaging, 30(11), 1996-2011.

[WAN 00] Wang JZ, Pathfinder: Region-based searching of Pathology Images using IRM, Proc. AMIA