Hierarchical Access Control and Content Protection in Medical Image Archives, Based on Inverse Pyramid Decomposition

ROUMEN KOUNTCHEV
Department of Radio Communications
Technical University of Sofia
Bul. Kl. Ohridsky 8, Sofia 1000
BULGARIA
rkountch@tu-sofia.bg
http://www.tu-sofia.bg

BARNA IANTOVICS
Petru Maior University
Str. N. Iorga,1
Tg. Mures
ROMANIA
barna_iantovics@yahoo.com
http://www.upm.ro

ROUMIANA KOUNTCHEVA
T&K Engineering
Mladost 3
Pob 12
Sofia 1712
BULGARIA
kountcheva_r@yahoo.com

Abstract: - In the paper is presented one new approach for management of medical databases with multi-layer access, based on the Inverse Pyramid Decomposition. This decomposition offers the ability for the development of interactive tools for multi-layer transfer of the processed visual information with consecutively quality improvement, selection of regions of interest, which to be directly accessed and represented with highest quality, and reliable content protection ensured by resistant and fragile watermarks embedding. The use of the Inverse Pyramid Decomposition permits insertion of multiple watermarks in the same file. The resistant watermarks are used to prove the documents authenticity, while the fragile watermarks hide preset Regions of Interest in the medical images which should be revealed by authorized users only, and prove any kind of editing of the protected visual content. The basic part of the database information which is at the low access level, could be used for various applications: disease history and treatment, statistics information, etc., and could support patients diagnostics, cure and telemedicine. The information, saved in the high access level(s) is accessible for authorized users only.

Key-Words: - Medical image databases, Management of image databases, Image content protection, Resistant watermark, Fragile watermark.

1 Introduction
Contemporary hospitals and healthcare institutions aim significant part of their efforts at better patients’ services. They comprise such basic applications as diagnostics, treatment, telemedicine, consultations with remote specialists, etc. For this, large amounts of medical information should be stored in huge information systems and easily accessed by authorized users. One of the most important implementations is the development of Electronic health records (EHR), which contain various multimedia objects (still images, multispectral and multi-view images, electronic documents, etc.). In medicine to date, virtually all Picture Archive and Communication Systems (PACS) retrieve images simply by indices based on patient name, technique, or some observer-coded text of diagnostic findings [1,2]. These systems connect hospital patient data with clinical data as the patient moves between providers and patient care establishments. Interoperable EHRs have the potential to promote access to more detailed and accurate patient

information at the time of treatment, to reduce medical errors and to improve the overall healthcare quality. The management of such databases should satisfy contradictory requirements: easy and reliable access, content protection, and many others. The usual approach is to use Digital Imaging and Communications in Medicine (DICOM) standard [3] (based on the JPEG standard). The images are compressed and stored and their accessibility and content protection depends on the medical database (MD) management. There are a number of uses for medical image databases, each of which would make different requirements on database organization. Classification of images into named or coded diagnostic categories may suffice for retrieving groups of images for teaching purposes. The so described techniques ensure flexible and reliable management of the stored medical information. Two main problems exist when the medical information is archived and stored: how to archive it efficiently, and how to ensure the needed content protection and confidentiality. The first
problem is solved using some kind of image and data compression. One of the most powerful contemporary tools for image archiving is the JPEG2000 image compression standard, which offers many features that support interactive access to large images [4,5], and the most famous standard, used for medical images, is DICOM [6]. This is a high-efficient compression, which ensures retained visual quality for the restored images, but it does not involve watermarking tools. The second problem (the image content protection) is based on some kind of watermarking, encryption, etc. The watermark insertion is usually performed in the frequency domain, which results in lower quality of the restored images, and the encryption techniques usually require significant computational power, especially when large files are processed.

In the paper is presented one new approach for hierarchical management of medical image databases, based on the Inverse Pyramid Decomposition (IPD), which offers various tools for layered transfer of the processed visual information with consecutively quality improvement, together with reliable content protection with resistant and fragile watermarks. The IPD offers lower computational complexity than the JPEG 2000 standard, together with direct accessibility to Regions of Interest (ROI) and image content protection. This approach is not in contradiction with the existing tools for database management. On the contrary, it complements them in the area of content protection and facilitates the establishment of hierarchical access control. The paper is arranged as follows: In Section 2, the basic principles of IPD are presented; in Section 3 is described the method for image content protection with watermark embedding; in Section 4 is presented the database management and Section 5 is the Conclusions.

2 Inverse pyramid decomposition
The 2D matrix [B], which corresponds to the digital image, could be represented using the IPD [9]. For this, the matrix is first divided into blocks of size 2\(^n\times2\(^n\). The sub-matrix for each block [B(2\(^n\))] is then decomposed as follows:

\[
[B(2^n)] = [\tilde{B}_0(2^n)] + \sum_{p=1}^{r-1} [\tilde{E}_p(2^n)] + [R(2^n)] \quad (1)
\]

for \(r<n-1\), where the number of decomposition components is \((r+2)\). Here [R(2\(^n\))] is a residual component, which is equal to zero for \(r=n-1\). Each component in Eq. 1 is a matrix of size 2\(^n\times2\(^n\), which corresponds to the decomposition layer \(p\).

The first decomposition component, [\(\tilde{B}_0(2^n)\)] calculated for the layer \(p=0\), is a coarse approximation of the block [B(2\(^n\))]. It is obtained through 2D inverse orthogonal transform (IOT) of the block [\(\tilde{S}_0(2^n)\)]:

\[
[\tilde{B}_0(2^n)] = [T_0(2^n)]^{-1} [\tilde{S}_0(2^n)] [T_0(2^n)]^{-1}, \quad (2)
\]

where \([T_0(2^n)]^{-1}\) is the matrix of the 2D OT, \([\tilde{S}_0(2^n)]\), of size 2\(^n\times2\(^n\);

\[
[\tilde{S}_0(2^n)] = FQ^{-1}_0 \{[\tilde{S}_0(2^n)]\} = FQ^{-1}_0 \{[S_0(2^n)]\}. \quad (3)
\]

\(FQ_0[\bullet]\) and \(FQ^{-1}_0[\bullet]\) are correspondingly the operators for filtration and quantization of \([S_0(2^n)]\) and for dequantization of \([\tilde{S}_0(2^n)]\) in the decomposition layer \(p=0\). In result of the operation, performed by \(FQ_0[\bullet]\), are selected and quantized the high-energy coefficients in the matrix\([S_0(2^n)]\), which define \([\tilde{S}_0(2^n)]\). In result of the performance of the operator \(FQ^{-1}_0[\bullet]\) and after the operation, represented in Eq. 2, is calculated the component [\(\tilde{B}_0(2^n)\)]. The term \([S_0(2^n)]\) in Eq. 3 is calculated after direct 2D OT of the matrix [B(2\(^n\))]:

\[
[S_0(2^n)] = [T_0(2^n)] [B(2^n)] [T_0(2^n)]. \quad (4)
\]

Here \([T_0(2^n)]\) is the 2D OT matrix, of size 2\(^n\times2\(^n\), which could be of any kind: (DFT, DCT, KLT, etc.), and whose inverse matrix is\([T_0(2^n)]^{-1}\). The retained decomposition components from Eq.1 are the approximating matrices \([\tilde{E}_p(2^n-p)]\) for levels \(p=1,2,...r\). They comprise sub-matrices\([\tilde{E}_p(2^n-p)]\) of size 2\(^n\times2\(^n\) for \(k_p=1,2,...,4^p\), obtained in result of the quad-tree division of \([\tilde{E}_p(2^n-p)]\). Each sub-matrix is defined as:

\[
[\tilde{E}_{p-1}(2^n-p)] = [T_p(2^n-p)]^{-1} [\tilde{S}_p(2^n-p)] [T_p(2^n-p)]^{-1} \quad (5)
\]

for \(k_p=1,2,...,4^p\), where: \(4^p\) is the number of the quad-tree branches in the level \(p\); \([T_p(2^n-p)]^{-1}\) is a matrix of size 2\(^{n-p}\times2\(^{n-p}\) in the level \(p\), used for the inverse 2D OT:

\[
[\tilde{S}_p(2^n-p)] = FQ^{-1}_p \{[S_p(2^n-p)]\} = FQ^{-1}_p \{[S_p(2^n-p)]\}; \quad (6)
\]

Each transform is defined by the equation:

\[
[S_p(2^n-p)] = [T_p(2^n-p)] [E_{p-1}(2^n)] [T_p(2^n-p)] \quad (7)
\]
Here $[T_p(2^{n-p})]$ is a matrix of size $2^{n-p} \times 2^{n-p}$ in the level $p$ for each block $[E^p_k(2^{n-p})]$ for $k_p=1,2,...,4^p$ in the difference matrix, defined by the relation:

$$
[E^p_{p-1}(2^{n-p})]=\begin{cases}
[B(2^p)]:[B_0(2^p)] & \text{for } p=1;

[B^2(2^{n-p})]:[B^2_{p-2}(2^{n-p})] & \text{for } p=2,3,...,r.
\end{cases}
$$

In result of the decomposition represented by Eq. 1, for each block $[B(2^n)]$ are defined the following coefficients:
- from the level $p=0$ - all non-zero coefficients in \([S'_0(2^n)]\);
- from levels $p=1,2,...,r$ - all non-zero coefficients \([S'_{kp}(2^{n-p})]\) for $k_p=1,2,...,4^p$.

The spectrum coefficients of same spatial frequency from all sub-blocks are then arranged in common massifs, and losslessly coded.

The processing of colour images is performed in similar way, but it requires 3 pyramids to be built, corresponding to the colour components.

On the IPD basis was created new digital format. The compressed image data consists of two parts – a header and coded data. The header contains information about the number of decomposition layers, the size of the initial sub-image, the kind of the used orthogonal transform, the number of transform coefficients for every layer, etc. The new format can also comprise additional information, necessary for the efficient arrangement and search in the medical database, for example: personal information about the patient: age, place of birth, etc.; information about the disease(s); etc.

3 Image watermarking

The image watermarking used in medical image databases should satisfy the following basic requirements:
- It should not decrease the image quality;
- It should resist the main fraud attacks;
- It should prove any kind of image editing.

Two watermarking methods were developed for the IPD: resistant and fragile. The resistant watermark is based on the use of the 2D Complex Hadamard Transform (2D-CHT). The basic property of the CHT is that the transform coefficients have real and imaginary part. The watermark data is inserted in the phases of selected spectrum coefficients, calculated using 2D-CHT with “arranged” Complex Hadamard matrix for the image matrix $[B(N)]$ [10]. The real part of these coefficients is not influenced by the watermark data and in result the inserted watermark is “transparent” (not noticeable). The watermark is resistant against compression, crop, etc., and is used to prove the authenticity of the visual document. The fragile watermark is inserted as separate decomposition layer and does not influence the restored image quality. It could be “transparent” or “hiding”. The transparent fragile watermark is used to prove any kind of image editing – even smallest changes in the watermark prove the image editing. The visible (hiding) watermark is visualized together with the protected image. When applied on the protected document, the watermark hides some significant part in it – for example, the Region of Interest (ROI). After visualization the ROI is “hidden” and should be revealed by authorized users only.

3.1 Resistant watermarking

The image matrix $[B(2^n)]$ of size $N \times N$ $(N=2^n)$ is first processed with direct 2D-CHT:

$$
[S(2^n)]=[CH(2^n)][B(2^n)][CH(2^n)].
$$

Here $[S(2^n)]$ is the matrix of the discrete image spectrum; $[CH(2^n)]$ - arranged matrix, defined by the natural Complex Hadamard matrix $[CH_0(2^n)]$ with elements:

$$
ch_0(t,q)=j^q h_0(t,q) \text{ for } t,q=0,1,...,2^n-1,
$$

$$
h_0(t,q)=\begin{cases}
1 & \text{for } n=2; \\
\sum_{i=0}^{\frac{n}{2}} \frac{1}{2^n} & \text{for } n=3,4,..,
\end{cases}
$$

The arranged transform matrix $[CH(2^n)]$ is obtained from the natural one, $[CH_0(2^n)]$ after rearranging its rows in such a way, that the number of sign changes for the elements in the row $q$ to be increased by one in the next row, $(q+1)$. The coefficients of the matrix $[S_0(2^n)]$ are:

$$
s_0(u,v)=\sum_{i=0}^{2^n-1} \sum_{k=0}^{2^n-1} B(i,k)e^{-j2\pi(au+vk)}h_0(u,i)h_0(v,k)
$$

for $u,v=0,1,...,2^n-1$, where $B(i,k)$ is the element of the original image $[B(2^n)]$. For the calculation of $s(u,v)$ coefficients, obtained using the $[CH(2^n)]$ matrix, is necessary to rearrange the $s_0(u,v)$ coefficients. Each coefficient is represented as:

$$
s_0(u,v)=s_{0,Re}(u,v) - js_{0,Im}(u,v)
$$

$$
=M_0(u,v)e^{-j\phi_0(u,v)},
$$

where:
From all spectrum coefficients are chosen the complex-conjugated couples \( s(u,v) \) and \( s^*(u,v) \) (with phases \( \phi(u,v) = -\phi^*(u,v) \) and modules \( |M(u,v)| = |M'(u,v)| \)). Every consecutive bit \( w_r(p) \) of the watermark data \( p \) is inserted in the phases of coefficients \( s(u,v) \) and \( s^*(u,v) \) only:

\[
\phi_{w_r(p)}(u,v) = \begin{cases} 
\phi(u,v) + \Delta, & \text{if } w_r(p) = 1; \\
\phi(u,v) - \Delta, & \text{if } w_r(p) = 0.
\end{cases}
\]  

Here \( \phi_{w_r(p)}(u,v) \) and \( \phi^*_{w_r(p)}(u,v) \) are the phases of the watermarked coefficients \( s_{w_r(p)}(u,v) \) and \( s^*_{w_r(p)}(u,v) \). The watermark data is represented by the binary sequence \( w_r(p) \) for \( r=1,2,...,R \) (\( R \) is the number of the watermark binary elements). The parameter \( \Delta \) is the angle, which defines the watermark “depth”, “transparency” and the resistance against pirates’ attacks. The sequence of bits \( w_r(p) \) is obtained after performing operation “XOR” both for each bit of the watermark and the corresponding bit from a pseudorandom sequence, which represents a secret (private) or public key, used for watermarking. In this case the autocorrelation function of the sequence \( w_r(p) \) is chosen to be of the kind “delta-pulse”. This ensures high accuracy for the watermark detection and extraction. In case that the currently processed complex spectrum coefficient has zero amplitude, the corresponding binary value of the watermark is omitted and the binary symbol from the pseudorandom sequence only remains, because “XOR” is not applied. In result, the errors in the extracted watermark elements are reduced, because the spectrum coefficients of zero amplitude have zero phases as well, and they are practically not suitable for watermark elements extraction. The coefficients of the rearranged matrix \( [S_w(2^n)] \) are:

\[
s_{w_r(p)}(u,v) = M(u,v)e^{-j\phi_{w_r(p)}(u,v)}
\]  

The matrix \( [S_w(2^n)] \) is processed with inverse 2D-CHT:

\[
[B_w(2^n)] = 4^{-n}[CH(2^n)]'[S_w(2^n)][CH(2^n)]',
\]

where \( [CH(2^n)]' = 2^n[CH(2^n)]^{-1} \).

The pixels of the watermarked image are:

\[
B_w(i,k) = \sum_{u=0}^{2^n-1} \sum_{v=0}^{2^n-1} s_w(u,v)e^{j[\phi(u,v) + \phi_{w_r(p)}(u,v)]}h_0(u,i)h_0(v,k)
\]  

for \( i, k = 0,1,...,2^n-1 \).

For the resistant watermark detection in unknown image are performed Eqs. (11-14), presented above. For this, first should be checked whether in the image had been inserted the watermark \( p \), which is one of the known \( D \) possible signs. For this is evaluated the mutual correlation \( C_{m,p} \) between watermarks \( m \) and \( p \), the first of which is one of the \( D \) possible, and the second is used for watermarking of the complex-conjugated coefficients \( s(u,v) \) and \( s^*(u,v) \) of the unknown image:

\[
C_{m,p} = \sum_{r=1}^{R} [\phi(u,v) + \Delta_r(p)]\Delta_r(m) = A(m) + B(p,m)
\]  

for \( p,m = 1,2,...,D \), where \( D \) is the number of searched watermarks; \( [\phi(u,v) + \Delta_r(p)] = \phi_{w_r(p)}(u,v) \) is the phase of the marked spectrum coefficient \( s_{w_r(p)}(u,v) \) of the matrix \( [S_w(2^n)] \), which contains the watermark data;

\[
\Delta_r(p) = \begin{cases} 
(1)^{w_r(p)}\Delta, & \text{if } w_r(p) = 1; \\
-\Delta, & \text{if } w_r(p) = 0,
\end{cases}
\]

\[
A(m) = \phi(u,v)\sum_{r=1}^{R} \Delta_r(m)\approx 0 \text{ for } R \gg 1,
\]

\[
B(p,m) = \sum_{r=1}^{R} \Delta_r(p)\Delta_r(m).
\]

In case that spectrum coefficients are not marked, \( \Delta_r(p) = 0 \) and \( C_{m,b} \approx 0 \); else:

\[
C_{m,p} \approx \begin{cases} 
\sum_{r=1}^{R} [\Delta_r(m)]^2 \approx R\Delta^2, & \text{if } m = p; \\
\sum_{r=1}^{R} \Delta_r(m)\Delta_r(p) \approx 0, & \text{if } m \neq p.
\end{cases}
\]  

The decision for the watermark detection is:

\[
p = \begin{cases} 
\text{Yes}, & \text{if } [C_{m,p}/R\Delta^2] \geq \theta; \\
\text{No}, & \text{in other cases.}
\end{cases}
\]

for \( m,p = 1,2,...,D \), where \( \theta \) is pre-defined threshold in the range \( 0 < \theta < 1 \). The so described watermark detection is “blind”, i.e. it does not need the original image.
For the watermark extraction is needed the original image. It is supposed, that the owner is the person, authorized to do this. After the phase spectrums of the original and the watermarked images had been calculated, the phases of the corresponding coefficients are subtracted and is defined the sequence, obtained after applying the “XOR” function on the watermark and the pseudorandom sequence, which is the encryption key. The watermark is obtained after performing “XOR” for phase differences sequences and the key.

### 3.2 Fragile Watermarking

IDP permits insertion of a different fragile watermark in every consecutive level, \( p \). The watermark could be a binary image, or data, overlaid on the processed decomposition level. The removal of the fragile “hiding” watermark is carried out using a password or other similar technique.

The fragile watermarking is performed working with the image data for the corresponding level. In this case, the data \( Z_p(r) \) is arranged in accordance with the relation:

\[
Z_p(r) = \begin{cases} 
X_p(r) & \text{for } r = 1, 2, \ldots, l_p; \smallskip 
W_p(r) & \text{for } r = l_p + 1, l_p + 2, \ldots, l_p + l_{wp},
\end{cases}
\]  

(23)

Here, \( W_p(r) \) is the data of the compressed watermark of length \( l_{wp} \) embedded in the decomposition layer (level) \( p \), using the password \( Y_p \). The password itself is a code of length \( l_p \) ≤ \( l_p \).

The number \( N_{wp} \) of the corresponding watermark for the layer \( p \) is defined by the relation:

\[
N_{wp} = l_p \oplus Y_p = \sum_{i=0}^{l_{wp}-1} (l_p^i \oplus y_p^i),
\]  

(24)

where \( l_p^i \) and \( y_p^i \) are the \( i^{th} \) binary digits of the numbers \( l_p \) and \( Y_p \), correspondingly, and with “\( \oplus \)” is noted the operation “exclusive OR”. The number \( N_{wp} \), corresponding to the watermark, is included in the header \( H_{wp} \) of the compressed data \( W_p(r) \).

The watermark image (prepared in advance) should be losslessly compressed. It is suitable to use a relatively small watermark (for example, 256x256 pixels) and to apply it over the original image as many times as necessary in the process of decompression, until the entire document (or the pre-selected ROI) is covered. The IDP permits binary watermarks of size 256 x 256 pixels to be losslessly compressed into files of size 500-800 bytes – depending on image contents. This size is negligible, compared to the size of the medical documents (X-ray images, scanned documents, etc.): even after compression, the obtained image files are usually very large, because the visual quality of the restored document has to be good and high compression ratios should not be used.

The next IDP layer creates another sequence \( Z_p(r) \), where one more watermark could be inserted.

### 4 Database management using the IPD decomposition

The IPD-based layered approach for image archiving permits the development of flexible software tools for image database management. The main idea is that any image in the database is visualized layer by layer with increasing resolution. The visualization starts with the coarse approximation of the archived image, which corresponds to the lowest decomposition layer. The next approximation (of higher quality) is visualized only in case that the user has a password or other kind of authorized access permission. Together with the better quality, the system reveals additional personal information. In case, that the image (or a part of it, containing a ROI) is hidden under a fragile watermark, it is visualized together with the watermark, which could be removed only if the password for the corresponding decomposition level is provided. The transparent fragile watermark is extracted using special software. In case that the fragile watermark had been changed, this proves image editing.

The block scheme of the image preparation for a database with hierarchical access is shown on Fig. 1. The image is archived layer by layer and the watermarks are inserted together with the image processing. The decomposition comprises \( N \) layers, but in practice are usually used 3 or 4 layers only. This approach offers significant abilities for efficient transfer and visualization, because the compression ratio in the lowest layer is usually 100 or higher, if 4 transform coefficients are used. The quality of the restored image is not high, but when visualized scaled down, it is good enough for the user to evaluate if he/she is interested with this information.

Additional advantage of the new decomposition is that it offers interactive abilities and permits the image creator to set ROI(s) in the archived image. The access request in the IPD-based system starts from the lowest decomposition layer and continues to the higher ones. The access permission for any layer needs a password. The information in the forbidden layers is not visualized and the image is restored with the quality of the highest permitted layer.
The proposed method for creation of medical databases with image content protection offers various tools for processing and archiving. The method is not in contradiction with the existing methods for database management. The main advantages of the new method are:

- It permits the creation of software tools for efficient management of medical databases;
- It offers flexible layered access to the archived information, depending on the user authorization;
- It ensures reliable content protection with multiple resistant and fragile watermarks;
- The layered approach for image processing permits the creation of general models for object description and representation. In the case, when RST-invariant transforms are used, the objects representation is RST-invariant[12];
- The proposed database management corresponds to the contemporary methods for content- and context-based data search;
- The proposed method has big potential for future investigations in the area of intelligent search in large image databases, which will support medical diagnostics and cure.

**Acknowledgement**

This work was supported by the Joint Research Project Bulgaria-Romania (2010-2012): “Electronic Health Records for the Next Generation Medical Decision Support in Romanian and Bulgarian National Healthcare Systems”.

**References:**