·安全技术· 文章编号:1000-3428(2016)05-0151-05 文献标识码:A 中图分类号:TP309.2

基于无损水印的 DICOM 文件头信息篡改检测

林 意,廖琴枝

(江南大学数字媒体学院,江苏 无锡 214122)

摘 要: 针对医学数字成像和通信(DICOM)文件头信息在公网上传输时可能会被非法篡改的问题,提出一种保护 DICOM 文件头信息的方法。将文件头信息作为图像像素灰度值进行处理,利用信息-摘要算法 5 构造的 Hash 函数生成文件头的消息摘要值,并将该消息摘要值作为水印,以可逆不可见的方式嵌入 DICOM 图像,使用提取水印与重新生成水印的差异进行文件头信息篡改检测。实验结果表明,该方法对文件头信息篡改具有极强的敏感性,可以检测到 1 bit 的篡改,认证过程计算简单,且准确性较高。

关键词: 医学数字成像和通信文件;医学图像;无损水印;Hash 函数;篡改检测

中文引用格式: 林 意,廖琴枝. 基于无损水印的 DICOM 文件头信息篡改检测[J]. 计算机工程,2016,42(5):151-155,162.

英文引用格式: Lin Yi, Liao Qinzhi. Tamper Detection of DICOM File Header Information Based on Lossless Watermarking[J]. Computer Engineering,2016,42(5):151-155,162.

Tamper Detection of DICOM File Header Information Based on Lossless Watermarking

LIN Yi, LIAO Qinzhi

(School of Digital Media, Jiangnan University, Wuxi, Jiangsu 214122, China)

【Abstract】 Aiming at the problem of illegally tampering of Digital Imaging and Communications in Medicine(DICOM) file header information when it transfers on the public network, a DICOM file header information tamper detection method is proposed. The method processes the file header information as image pixels, and generates the watermark of the file header information with Hash function constructed by Message-Digest Algorithm 5(MD5). The watermark of the image is embedded in DICOM image as an reversible and invisible way. The difference between the extracted watermark and the regenerated watermark is using for tamper detection of the DICOM file header. Experimental result indicates that, this method is highly sensitive to the file header information tampering. Even 1 bit change can be detected, the certification process is simple and the accuracy is high.

【Key words】 Digital Imaging and Communications in Medicine(DICOM) file; medical image; lossless watermark; Hash function; tamper detection

DOI: 10.3969/j.issn.1000-3428.2016.05.026

1 概述

与一般图像文件的文件头不一样,医学数字成像和通信(Digital Imaging and Communications in Medicine,DICOM)[1]文件头是整个 DICOM 文件中最复杂的部分,它包含一些非常有用的信息,如患者姓名、器官部位、图像模态等。这些信息涉及到医院的知识产权,不允许随便修改。虽然目前各个医院系统之间是相互独立的,且今后医疗信息会共享,于是信息在公网上传输时可能被非法篡改[2-4],因此,保护这些信息的安全问题就变的极为重要。

然而,目前绝大部分的篡改检测是针对 DICOM 图像部分[5-7],很少见到研究除图像像素部分外的 DICOM 文件头中信息安全的相关文献出现,而 DICOM 文件在公网上传输时,文件头信息就暴露在外,这些重要信息极易被修改,例如病人的名字、图像的模态等,而当使用者并未察觉这些信息被非法修改过,就会导致医疗信息的错误使用,引起医疗事故、医疗纠纷等。

针对这个问题,本文提出一种适用于保护 DICOM 文件头信息的方法,该方法将所有文件头字节进行处理,利用信息-摘要算法 5(Message-Digest Algorithm 5,MD5)构造的 Hash(散列)函数生成的图像消息摘要值作为水印,并以可逆不可见[8-9]的方

作者简介: 林 意(1963-),男,副教授,主研方向为信息安全、隐私保护;廖琴枝,硕士研究生。

收稿日期: 2015-04-17 **修回日期:** 2015-06-09 **E-mail:** linyi01@vip.sina.com

式嵌入 DICOM 图像部分,以进行之后的文件头信息篡改检测。

2 DICOM 文件简介

DICOM 标准是美国放射学会和美国电器制造商协会组织制定的标准,包括了医学的数字成像与通信 2 个方面,目前已被医疗设备生产商和医疗界广泛应用。DICOM 文件是根据 DICOM 标准而存储的医学文件,它的后缀名为. dcm,一般由一个 DICOM 文件头和一个 DICOM 数据集合组成[10]。

与一般图像文件的文件头不一样,DICOM 文件的文件头包括很多有用的信息,这些信息用来标识数据集合,是整个 DICOM 文件中最复杂的部分[11]。DICOM 文件必须包含 DICOM 文件头,一般 DIOCM 文件头的最开始是文件前言,由 128 个 00H 字节组成。接下来是 DICOM 前缀,它是一个字符串“DICM”,长度为 4 Byte,该值用来判断一个图像文件是否为 DICOM 文件。在文件前言和前缀之后,是一些很有用的信息,这些信息是 DICOM 文件区别于一般文件的主要部分,如与文件相关的信息,包括文件名、生成日期、类型、大小、规格等;如与患者相关的信息,包括患者姓名、性别、年龄、医院名称、扫描时间等;如与设备相关的信息,包括设备的序列号、生产厂商、名称等;与图像相关的研究信息,包括图像模态,如计算机断层扫描(Computed Tomography, CT)、磁共振成像(Magnetic Resonance Imaging, MRI)等;器官部位,如心脏、脑颅等;还有扫描时的参数设置,如曝光时间、扫描层面的位置、滤波器的类型等。具体如表 1 所示。

表 1 DICOM 文件头中的有用信息(部分)

标签号	标签名	描述	实例
(0008,0060)	Modality	模态	MR
(0010,0010)	Patient Name	患者姓名	AB
(0010,0020)	Patient ID	患者编号	20100309004
(0010,0040)	Patient Sex	患者性别	M
(0010,1010)	Patient Age	患者年龄	32

DICOM 数据集合是由 DICOM 数据元素按照一定顺序排列组成的[12]。数据元素(Data Element)是 DICOM 文件中最基本的单元,它主要由 Tag(标签)、值类型描述(Value Representation,VR)、值长度(Value Length)和值域(Value Field)4 个部分组成。DICOM 医学图像的像素部分就包含在标签名为(7FE0 0010)的数据元素值域中。

3 DICOM 文件头信息水印算法实现

本文提出一种基于无损数字水印的 DICOM 文件头信息篡改检测方法,此方法大致分为:

(1)新建一个空白图像,把 DICOM 文件头所有字节作为此图像像素值填入。

(2)利用 MD5 算法构造的 Hash 函数生成此图像的消息摘要值。

(3)使用基于固定位置的可逆整数变换将消息摘要值作为水印嵌入 DICOM 图像中。

(4)提取嵌入的水印值进行 DICOM 文件头信息篡改检测,同时恢复 DICOM 图像像素值。

DICOM 文件头认证信息的生成和嵌入过程如图 1 所示。

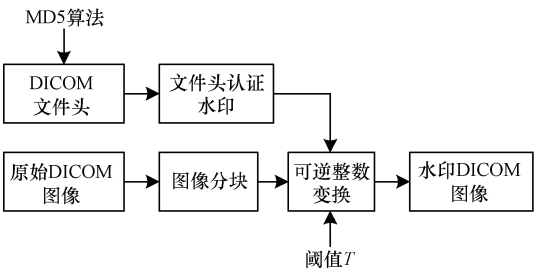


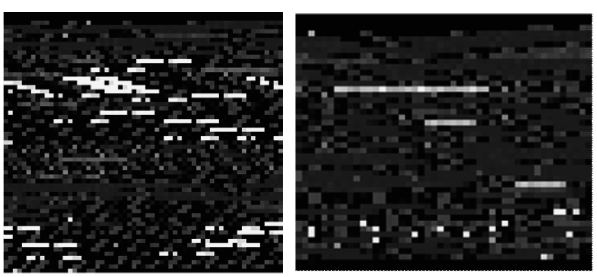
图 1 文件头认证水印生成及嵌入过程

3.1 DICOM 文件头认证信息生成过程

3.1.1 文件头字节填入空白图像的过程

DICOM 文件在生成以后,在用于共享时,即使授权的医院或医生一般也不允许修改相关信息,医生只是借助该影像来辅助医疗,所以,可以将整个文件头信息一起进行处理。

针对一个具体的 DICOM 文件实例,首先获取整个文件的大小,然后计算得出 DICOM 图像像素部分的大小,以整个文件的大小减去 DICOM 图像像素部分的大小得到文件头的大小,将整个文件头以字节的形式读入内存,把它们填入某空白图像中。这样能保证整个文件头的字节值不变,也就是内容不变又能描述全部 DICOM 文件头信息。如图 2(a)是采用的实验示例 1 的文件头图片,大小为 3 686 Byte,图 2(b)是示例 2 的文件头图片,大小为 2 028 Byte。



(a)示例1 DICOM文件头图片 (b)示例2 DICOM文件头图片

图 2 示例对象 DICOM 文件头图片

3.1.2 文件头消息摘要值的生成

本文采用 MD5 算法构造的 Hash 函数生成文件头图片的消息摘要值。Hash 函数具有高度敏感性,

且基于 MD5 算法的 Hash 函数具有数字指纹的特性,它是目前应用最广泛的一种文件完整性校验和(Checksum)算法。

Hash 就是把任意长度的输入,通过散列算法,变换成固定长度的输出,该输出就是散列值。

MD5-Hash 算法的原理[13]是算法的输入为任意长度的消息,首先把输入的消息分为 512 bit 的数据块,然后把每一个 512 bit 的数据块划分为 32 bit 的子块,共 16 个子块,每个 32 bit 的子块分别进行处理,经过计算后,算法的输出结果为 128 bit 的摘要。与一般的加密算法不同,Hash 算法的安全性高,且它是一个不可逆的单向函数,不同的输入几乎不可能得到相同的 Hash 结果。因此,当 MD5 输入发生任何微小变化时,即 DICOM 文件信息发生任何改变,则生成的 DICOM 文件头信息摘要必然发生改变,敏感性高的 Hash 函数使得文件头信息的篡改检测非常直观,如果重新生成的文件头水印与提取的嵌入水印不一致,则说明 DICOM 文件头已经被篡改。该算法计算效率高,对图像的篡改敏感性高,适合保护 DICOM 文件头信息的完整性。

3.2　认证水印的嵌入

本文使用基于固定位置的可逆整数变换将 DICOM 文件头的消息摘要值作为水印值嵌入 DICOM 图像中。基于固定位置的可逆整数变换[14]分为正变换和逆变换,正变换用来嵌入水印,逆变换用来提取水印和还原原始图像,是具有代表性的空域算法之一。该算法实现简单,且嵌入容量大,能抵抗一般攻击,而且是无损不可见的,适用于高质量要求的医学图像应用。水印嵌入的具体步骤如下:

(1)首先按照从左到右、从上到下的扫描顺序扫描原始 DIOCM 图像 I,将 I 划分成 2×2 互不重叠的子块。对每个块中的 4 个像素,选取左上角的第一个像素作为参考像素 ref,整个过程中参考像素的值是不变的。

(2)对于图像块中除参考像素 ref 之外的任一像素 a,根据 a 与 ref 的关系嵌入水印。如果满足 $|a-ref|<T$,那么像素 a 可嵌入 1 bit 信息,a 的值按式(1)修改。否则转步骤(3)。

$$a_w=\begin{cases}a+T & msg(i)=1\\ a-T & msg(i)=0\end{cases} \tag{1}$$

其中,T 表示嵌入水印的阈值,这里 $T=5$,T 的大小可以根据具体情况进行调整,T 的值越大,水印嵌入的容量就越大,不过图像的失真也相应会越大,它可取的最大值为大于所有 $|a-ref|$ 的最小整数值;a_w 表示嵌入水印后的像素值;msg 代表待嵌入的 128 位文件头认证信息;i 表示待嵌入二进制流 msg 的下标,必须满足 $1\leqslant i\leqslant128$。

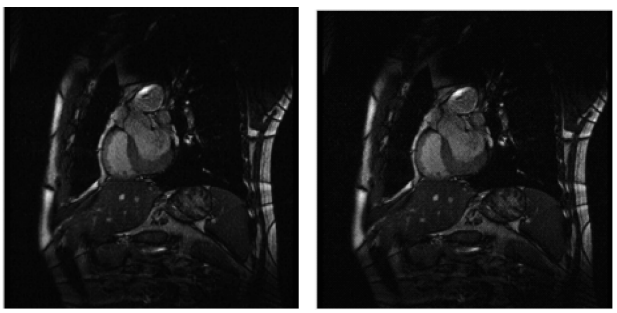
(3)对于 $|a-ref|\geqslant T$,那么 a 不能嵌入信息,a 的值按式(2)修改。

$$a_w=\begin{cases}a+T & a\geqslant ref\\ a-T & a<ref\end{cases} \tag{2}$$

(4)重复执行上述步骤(2)和步骤(3),所有的水印均被嵌入或者所有的图像块均被处理完就截止,得到水印 DICOM 图像 I'。

为了防止溢出,所有像素点的值必须满足 $0\leqslant a_w<256$。对于溢出像素点,进行像素点的记录,将记录作为水印的一部分进行嵌入。

嵌入水印后的 DICOM 图像显示与嵌入水印前的 DICOM 图像几乎是一样,肉眼看不出来区别,不会对图像的应用造成较大影响。如图 3 是示例 1 嵌入水印前后的 DICOM 图像对比。



(a)示例1原始DICOM图像　(b)嵌入水印后示例1的DICOM图像

图 3　嵌入水印前、后示例 1 的 DICOM 图像对比

3.3　水印提取、图像恢复与篡改检测

合法使用者在使用共享的 DICOM 文件时,首先得先检测该 DICOM 文件头是否被人篡改,再加以使用,避免不必要的事故和纠纷。水印提取、数据恢复以及 DICOM 文件头信息的篡改检测过程如图 4 所示。

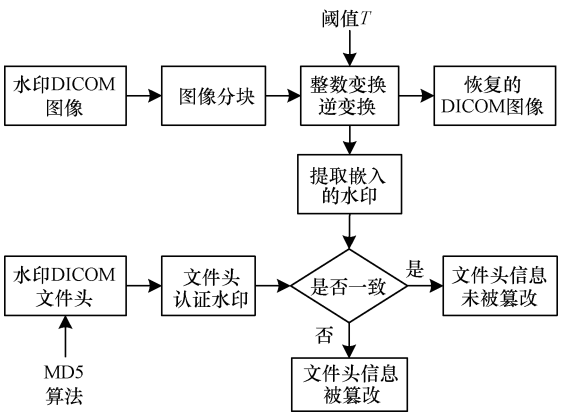


图 4　水印提取、数据恢复及篡改检测过程

本文针对 DICOM 文件头信息部分进行篡改检测,在得到嵌入水印的 DICOM 文件后,首先提取嵌入的水印值并恢复图像。具体步骤如下:

(1)首先按照与嵌入时相同的扫描顺序,扫描水印 DICOM 图像 I',将 I'划分成 2×2 互不重叠的块。对每个块中的 4 个像素,选取左上角像素为参考像素 ref。

(2)对于图像块中除参考像素 ref 之外的任一像素 a_w,将其与参考像素 ref 进行比较,根据它们的关系恢复图像像素值,如式(3)所示。

$$a_r = \begin{cases} a_w - T & a_w \geqslant ref \\ a_w + T & a_w < ref \end{cases} \tag{3}$$

其中,a_r为恢复后的像素值。

(3)判断 a_r与 ref 的关系,如果 $|a_r - ref| < T$,则按式(4)提取水印信息,否则不能提取水印信息,继续处理块中剩下的像素。

$$msg(i) = \begin{cases} 1 & a_w \geqslant ref \\ 0 & a_w < ref \end{cases} \tag{4}$$

(4)重复执行上述步骤(2)和步骤(3),当所有块被处理完毕或者水印已经提取完毕时停止,得到提取出的水印序列 msg'。

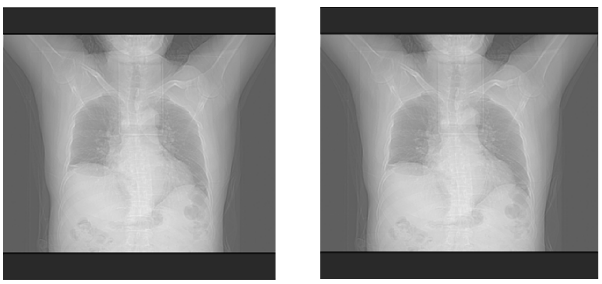
然后用嵌入时相同的方式计算出水印 DICOM 文件头的消息摘要值 msg。将 2 个水印值 msg 与 msg'进行比较,是否一致,若一致,则表示 DICOM 文件头信息并未被人篡改,可以安全使用,若不一致,则表示 DICOM 文件头信息被篡改,不宜使用。

例如水印示例 1 的 DICOM 文件头信息没有被篡改,按嵌入时的方式生成水印示例 1 的 DICOM 文件头的 Hash 消息摘要值为“f172d8b9e1940f799d70f0708e4eba44”(Hash 值的十六进制表示,下文的 Hash 值都用十六进制表示),且从水印示例 1 的 DICOM 图像部分提取的水印序列为“f172d8b9e1940f799d70f0708e4eba44”,对比后完全一致,可知文件头信息未被篡改。而当水印示例 2 的 DICOM 文件头中某一项信息被修改时,例如修改病人的名字,则生成的 DICOM 文件头的 Hash 消息摘要值为“a66050223177eae0c0642e10da7f5436”而从水印示例 2 的 DICOM 图像部分提取的嵌入的水印值为“55d689bf43e26b05a3d5941139cb815f”,对比可知这 2 个水印值是明显不一致的,由此判断文件头信息是被修改过的。

由此表明,本文方法对篡改具有极强的敏感性,且认证过程简单、准确性很高。采用的水印嵌入算法计算简单,且嵌入过程可逆,可以恢复医学图像的原始像素值,能抵抗一般的攻击,适用于 DICOM 文件头的保护。

4 实验结果分析

本文采用 Matlab 软件进行模拟仿真实验,实验选择了 20 幅 DICOM 标准的原始医学图像作为实验对象,限于篇幅,随机选取其中 2 幅为例。示例 1 为 256×256 像素的 MR 图像,DICOM 文件头大小为 3 686 Byte,文件头信息图片的 Hash 消息摘要值为“f172d8b9e1940f799d70f0708e4eba44”,嵌入前、后的 DICOM 图像对比见图 3。示例 2 为 512×512 像素的 CT 图像,DICOM 文件头大小为 2 028 Byte,文件头信息的消息摘要值为“55d689bf43e26b05a3d5941139cb815f”,嵌入前、后的 DICOM 图像对比见图 5。



(a)示例2原始DICOM图像 (b)嵌入水印后示例2的DICOM图像

图 5 嵌入水印前、后示例 2 的 DICOM 图像对比

4.1 水印不可见性实验

图 3 和图 5 分别表示了示例 1 和示例 2 嵌入水印前和嵌入水印后的 DICOM 图像对比。

由图可见,嵌入水印后的 DICOM 图像显示与嵌入水印前的 DICOM 图像几乎是一样,肉眼看不出来区别,水印图像的视觉质量良好,适合于高质量要求的医学图像,并且最后恢复出的图像和原始图像毫无差异,证明了算法的可行性。

4.2 嵌入水印图像的质量

结合均方误差(Mean Square Error,MSE),对图像的质量采用峰值信噪比(Peak Signal to Noise Ratio,PSNR)来进行评价。其计算公式如下:

$$M_{\text{MSE}} = \frac{\sum_{i}^{M}\sum_{j}^{N}(I(i,j) - I'(i,j))^2}{M \times N}$$

$$P_{\text{PSNR}} = 10 \times \lg \frac{(2^p - 1)^2}{M_{\text{MSE}}} \tag{5}$$

其中,M,N 分别表示原始载体图像的长和宽;I 表示原始图像;I'表示嵌入水印后的图像;p 为图像像素位深。

水印图像的视觉质量与阈值 T 的选取相关,由于医学图像不允许大的失真,本文设定 $T \leqslant 5$。最坏的情况就是所有像素值均被调整了 5 个灰度级,根据式(5)的计算得到最小的 $P_{\text{PSNR}} = 34.15$ dB。而且通过计算嵌入水印后的示例 1 图像和示例 2 图像的 PSNR 值也可以看出,水印的嵌入对医学图

像的质量影响很小,因此,可以看出本文所采用的无损水印算法在满足不可见性要求的同时具有较高的峰值信噪比,适用于 DICOM 医学文件的文件头信息认证。

4.3　篡改检测实验

Hash 算法是单向函数,它也是不可逆的函数,安全性高,不同的输入几乎不可能得到相同的 Hash 结果。因此,当 DICOM 文件信息发生任何改变时,则生成的 DICOM 文件头信息摘要必然发生改变,敏感性高的 Hash 函数使得文件头信息的篡改检测非常直观。

为了验证算法的有效性,本文对实验对象的一些基本文件头信息进行修改,修改程序采用 Matlab GUI 来实现[15],程序界面如图 6 所示。下面展示示例 2 的篡改检测实验,原始文件头的 Hash 值为“55d689bf43e26b05a3d5941139cb815f”,具体的修改项及篡改后文件头 Hash 值如表 2 所示。

图 6　基于 Matlab GUI 的文件头信息修改程序界面

表 2　示例 2 DICOM 文件头篡改检测

描述	原始信息	篡改后信息	篡改后 Hash 值
模态	CT	MR	f8fcd81bc145a6132a6aae6278a4a4db
患者姓名	AA	BB	a66050223177eae0c0642e10da7f5436
患者出生日期	19490207	19940207	c469750f351337012e84550bc4d64760
患者性别	M	F	1b08e0460a0d634f9e40fbda5693cbd1
患者年龄	60	20	5604b59cd767798ce957de4843e75aee

篡改时只篡改对应一项,而保持其他项内容不变。从水印示例 2 的 DICOM 图像中提取的 Hash 水印值都为“55d689bf43e26b05a3d5941139cb815f”,对比可知,文件头信息被篡改,且每一项的篡改都能检测出来。从表中可以看出,虽然只修改了一点点内容,但是文件头的 Hash 值变化很大。说明本文算法能正确检测出 DICOM 文件头信息是否被篡改,且本文算法运行效率高,能够有效保护 DICOM 文件头中的信息安全,同时保护了医院的知识产权不受侵害。

5　结束语

基于 Hash 函数和无损不可见水印算法,本文提出一种适用于保护 DICOM 文件头信息的方法。实验结果表明,该方法能检测出对 DICOM 文件头信息很小的篡改,且准确性很高。由于算法是针对整个 DICOM 文件头进行处理的,并未具体定位到文件头中某项数据元素的数据域值被篡改,因此今后将对 DICOM 文件头信息具体篡改定位和恢复方面进行研究,使之更符合医院及研究人员的需要。

参考文献

[1] 王甜甜,李国侠,庞　浩,等. 基于 Matlab 软件的 DICOM 图像的信息提取[J]. 中国医疗设备,2013,28(12):61-62.

[2] Luiz S F,Sergio S L,Paulo M B. Providing Integrity and Authenticity in DICOM Images:A Novel Approach[J]. IEEE Transactions on Information Technology in Biomedicine,2009,13(4):582-589.

[3] 邓小鸿,陈志刚,毛伊敏. 基于无损水印的医学图像篡改检测和高质量恢复[J]. 中国图象图形学报,2014,19(4):583-591.

[4] 梁涤青,陈志刚,邓小鸿. 基于混沌加密的医学图像安全共享方案[J]. 小型微型计算机系统,2016,37(1):162-167.

[5] Guo Xiaotao,Zhuang Tiange. Lossless Watermarking for Verifying the Integrity of Medical Images with Tamper Localization[J]. Journal of Digital Imaging,2009,22(6):620-628.

[6] Li Chunlei,Wang Yunhong,Ma Bin,et al. Tamper Detection and Self-recovery of Biometric Images Using Salient Region-based Authentication Watermarking Scheme[J]. Computer Standards and Interfaces,2012,34(4):367-379.

[7] Tian Lihua,Zheng Nanning,Xue Jiaru,et al. An Integrated Visual Saliency-based Watermarking Approach for Synchronous Image Authentication and Copyright Protection[J]. Signal Processing:Image Communication,2011,26(8):427-437.

[8] Deng Xiaohong,Cheng Zhigang,Zeng Feng,et al. Authentication and Recovery of Medical Diagnostic Image Using Dual Reversible Digital Watermarking[J]. Journal of Nanoscience & Nanotechnology,2013,13(3):2099-2107.

(下转第 162 页)

保证交互认证过程的安全性。虽然本文提高了用户存储密钥的安全性,但未减少用户存储的密钥数。因此,构建安全性和效率都高的方案,并减少用户存储的密钥存储数量将是下一步需要研究的问题。

参考文献

[1] Fan Rong,He Daojing. An Efficient and DoS-resistant User Authentication Scheme for Two-tiered Wireless Sensor Networks[J]. Journal of Zhejiang University: Science C, 2011,12(7):550-560.

[2] Jiang Qi,Ma Jianfeng,Li Guangsong,et al. An Enhanced Authentication Scheme with Privacy Preservation for Roaming Service in Global Mobility Networks[J]. Wireless Personal Communications,2013,68(4):1477-1491.

[3] Pippal R S,Jaidhar C D. Secure Key Exchange Scheme for IPTV Broadcasting[J]. Informatica,2012,36(1):47-52.

[4] Liao Yipin,Wang Shenshang. A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment[J]. Computer Standards & Interfaces,2009,31(1):24-29.

[5] Chen Te-Yu,Hwang Min-Shiang,Lee Cheng-Chi,et al. Cryptanalysis of a Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment[C]// Proceedings of the 4th International Conference on Innovative, Computing, Information and Control. Washington D. C.,USA: IEEE Computer Society,2009: 725-728.

[6] Hsiang C, Shih W K. Improvement of the Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment[J]. Computer Standards & Interfaces,2009,31(6):1118-1123.

[7] Lee C C, Lin Tsung-Hung, Chang Ruixiang. A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment Using Smart Cards[J]. Expert Systems with Applications, 2011, 38(11): 13863-13870.

[8] Li Xiong,Xiong Yongping,Jian Ma,et al. An Efficient and Security Dynamic Identity Based Authentication Protocol for Multi-server Architecture Using Smart Cards[J]. Journal of Network and Computer Applications, 2012, 35(2):763-769.

[9] Xue Kaiping,Hong Peilin,Ma Changsha. A Light Weight Dynamic Pseudonym Identity Based Authentication and Key Agreement Protocol Without Verification Tables for Multi-server Architecture[J]. Journal of Computer and System Sciences,2012,80(1):195-206.

[10] 万 涛,廖维川,马建峰. 面向多服务器架构的认证协议分析与改进[J]. 西安电子科技大学学报,2013, 40(6):174-179.

[11] Wang Bin,Ma Maode. A Smart Card Based Efficient and Secured Multi-server Authentication Scheme[J]. Wireless Personal Communications,2013,68(2):361-378.

[12] Ravi S P, Jaidhar C D, Shashikala T. Robust Smart Card Authentication Scheme for Multi-server Architecture[J]. Wireless Personal Communication,2013,72(1):729-745.

[13] Guo Dianli,Wen Fengtong. Analysis and Improvement of a Robust Smart Card Based-authentication Scheme for Multi-server Architecture[J]. Wireless Personal Communications,2014,78(1):475-490.

[14] Burrows M, Abadi M, Needham R M. A Logic of Authentication[J]. Proceedings of the Royal Society of London,Series A: Mathematical and Physical Sciences, 1989,426(1871):233-271.

[15] Kessler V,Wedel G. AUTLOG——An Advanced Logic of Authentication[C]//Proceedings of IEEE Computer Security Foundations Workshop VII. Franconia, USA: IEEE Press,1994:90-99.

[16] Kemal B, Nazife B. One-time Passwords: Security Analysis Using BAN Logic and Integrating with Smart Card Authentication[J]. Lecture Notes in Computer Science,2003,2869:794-801.

编辑 刘 冰

(上接第 155 页)

[9] Eswaraiah R,Reddy E S. Robust Medical Image Watermarking Technique for Accurate Detection of Tampers Inside Region of Interest and Recovering Original Region of Interest[J]. IET Image Processing,2015,9(8):615-625.

[10] 微笑的艾米. DICOM 医学图像文件格式[EB/OL]. [2015-03-08]. http://blog. csdn. net/okaimee/article/details/5736710.

[11] 费晓璐. 医学影像 DICOM 格式测试方法探讨[J]. 中国医学影像技术,2012,28(1):160-163.

[12] 邱明辉,刘海一. DICOM 标准医学图像文件解析及工具软件的研制[J]. 中国医学影像学杂志,2009, 17(5):368-373.

[13] 钟晓燕,冯前进,陈武凡,等. 基于 Hash 函数敏感性的医学图像精确认证[J]. 中国图象图形学报,2008, 13(2):204-208.

[14] 尚冠宇,郭凡新,邓小鸿. 基于采样预测和差值变换的医学图像可逆水印算法[J]. 计算机应用与软件, 2012,29(6):21-25.

[15] 赵媛媛,张进禄,陈大兴,等. 基于 Matlab GUI 的 DICOM 文件头信息处理[J]. 中国医学影像技术, 2012,28(11):2075-2078.

编辑 刘 冰