Analysis of the adoption of security headers in HTTP

William J. Buchanan, Scott Helme, Alan Woodward

IET Information Security 12 (2018) 118–126

HTTP安全报头的使用分析

William J. Buchanan, Scott Helme, Alan Woodward

IET Information Security 12（2018）118-126

摘 要

随着网络系统内威胁数量的增加，需要采取更加综合的方法确保从服务器到客户端执行安全策略。这些政策旨在阻止中间人攻击，代码注入等。本研究分析了HTTP响应中使用的一些最新的安全选项，并对其进行了扫描在HTTP响应中实现Alexa Top 100万个网站。这些扫描的选项包括：内容安全性策略，HTTP的公钥固定扩展，HTTP严格传输安全性和HTTP头字段X-frame-options，以便了解这些选项对最受欢迎网站的影响。结果表明，虽然执行参数不断增加，但仍未在许多顶级网站上实施。随着这一点，研究显示了采用Let's Encrypt数百万个网站的数字证书，以及评估安全质量的方式头。

关键字：超媒体；公钥加密；传输协议；网站。

# 1 引言

使用HTTP，我们有一个请求，比如GET请求，和服务器响应一个响应。 这些响应包含标题包含参数列表中定义的信息键：值对[1]。 有许多标准的应用程序层用于交换信息的协议，包括HTTP[1]，SMTP [2]，FTP [3]和DNS [4]。 这些规格是通常被编写为支持简单的基于文本的消息交换。其中一些是无状态的，例如DNS和HTTP其他人，如SMTP和FTP，则需要创建会话命令和响应。 当时，安全也经常是后想，以及应用层协议的位置通过增加安全套接字来提高安全性层（SSL），例如HTTPs [5]。

虽然SSL和传输层安全（TLS）纯粹受保护消息交换的内容，增加了CSP - 内容安全策略 - [6]集成了一套策略语言Web资源上的内容限制以及服务器的位置将该政策传送给客户，以便执行该政策。新还添加了安全扩展以防止中间人（MITM）攻击，例如公钥锁定扩展对于HTTP（HPKP）[7]并允许站点自行关联与特定的密码公钥并从而防止伪造数字证书。在HTTP严格传输安全性内（HSTS）[8] Web服务器可以要求客户端（及其关联的网页浏览器）只能通过安全的方式与它进行交互连接（如使用HTTPS）。在2013年，RFC 7034定义HTTP头域X-frame-options（XFO）[9]，它保护网页针对点击劫持的应用程序，以及针对整合的应用程序来自不可信来源的代码。重点再次放在服务器上通知客户其策略和配置选项。

本文分析了这些新安全功能的用法在Alexa Top 1 Million网站内，以确定影响推出安全响应头文件。 可以看出，在如图1所示，响应头包括：CSP，content-securitypolicy-仅报告（CSPRO），公钥管理（PKP），公钥管理 - 仅报告（PKPRO），仅X内容类型，XFO和X-Xssprotection（XXP）。 随着这一点，采用Let's Encrypt[10]显示了使用免费数字的一个有趣的举动证书。 因此，分析也将考虑采用它，并查看百万个网站是否使用Let's Encrypt证书权威（CA）。

# 2 背景

虽然SSL / TLS纯粹保护数据交换的内容，CSP [1]的增加提供了可以设定的策略语言Web资源上的内容限制以及服务器的位置将该政策传送给客户，以便执行该政策。 新安全扩展也被添加以防止MITM攻击，如HPKP [11]，它允许一个网站与自己联系在一起特定的密码公钥并防止伪造数字证书。 通过HSTS [12]，Web服务器可以要求a客户端（及其相关的网络浏览器）应该只与它交互通过安全连接（如使用HTTPS）。

RFC 7034添加了HTTP头字段XFO [13]，它可以保护针对点击劫持的网络应用程序，以及整合之中来自其他网页的内容。 重点再次放在服务器上告诉客户其策略和配置选项。 响应头文件包括：CSP，CSPRO，PKP，PKPRO，仅X内容类型，XFO和XXP。

总的来说，网络侧重于一个同源策略[14]，其中的包含在一个来源中的脚本仅被允许访问数据在那个原点之内，因此每个原点都与其他原点隔离。不幸的是，这与开发者以及攻击者过度地限制了开发者使用清晰的技巧从其他域注入恶意代码。许多媒体网站也经常使用其他内容和脚本并且会努力支持限制他们的内容到他们自己的网站。 来自其他站点的代码的集成可能会导致以跨代码脚本（XSS）攻击为代码的问题在网页内往往是完全可信的。 在CSP中，我们拥有许多防止XSS的方法。 有了这个CSP支持资源的多个策略，可以在Content-安全策略头或在<meta>元素内，例如[14]：

Content-Security-Policy: default-src https:

<meta http-equiv="Content-Security-Policy’content="default-src https:">

CSP最强大的功能之一是定义白名单供客户使用。 因此常见的问题是a浏览器将信任页面中的所有代码，以便来自其他站点的内容是可信的，因此，在CSP内部，Content-Security-策略HTTP标头用于定义可信来源，以及没有其他内容来源可以使用。 例如，如果我们只需https://asecuritysite.com上的代码我们就可以使用：

Content-Security-Policy: script-src ‘self’

https://asecuritysite.com

在这种情况下，我们相信我们自己的源代码（'self'）和来自https://asecuritysite.com的任何脚本。 代码被注入时从另一个来源进入页面，会出现错误。 对于内容，我们也可以限制图片，媒体，插件，样式表和其他对象可以从使用安装指示：

其中，x（t），Y（t）和Z（t）为颗粒在时间t时的图像中的位置。其下一图像中的位置是x（T + DT），γ（T + DT）和z（T + DT）。

PTV试图跟踪单个粒子。这种方法通常假设本地速度梯度是相对静止的，并且该颗粒在图像之间的运动不会超出它们的平均间隔。PTV因此通常用于当粒子分布相对分散的情况。PTV是相对准确的，但匹配颗粒效率低。在本文中，这两种算法根据在所述询问窗口的功能被选择来匹配粒子图像。

# 3.古典双目视觉模型

在本文中使用的3DPIVS是双目视觉系统。它包括两台CCD照相机用于同步捕获流体图像和重建三维图像[5-10]。根据CCD的位置，双目视觉可分为平行光轴模型和相交光轴模型。并联的相机可以直接使用视差信息来计算点的坐标空间，但相交相机需要整改在匹配过程之前。

## 3.1.平行光轴模型

两个具有平行光轴的摄像头，具有相同的焦距和内部参数。如果沿着X轴移动一定距离，两个摄像头的位置可以重合。两个光学中心之间的线通常被称为基线。在图2中，P是在空间中的一个给定的点； O1和O2分别是两个相机光学中心。

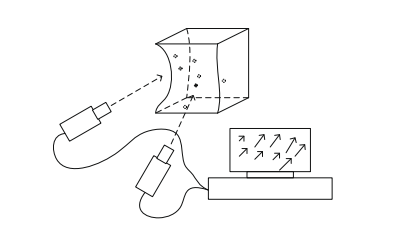


图1. 3D粒子图像测速系统

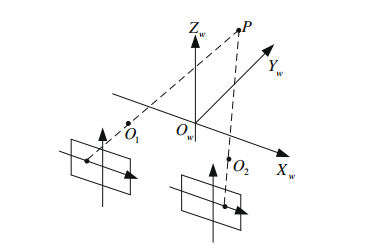


图2. 平行立体视觉

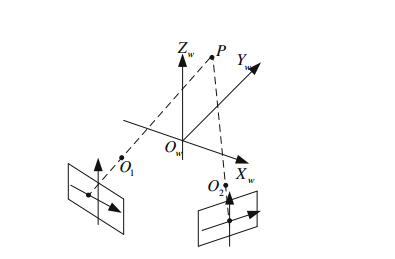


图3. 相交立体视觉

## 3.2.相交光轴模型

在平行光轴系统，公共视野是有限的。为了增加两个照相机的公共视图区域其光轴需要在实践中相交。图 3中，P是在空间中的一个给定的点; O1和O2分别是两个相机光学中心。

# 4. PIV的双目视觉模型

因为在PIV的角度测量，级联和混乱的现象是不可避免的。如图4所示，在世界系统的对象成像于两个照相机平面。定义S和F为CCD1和CCD2的影像集，那么我们可以得到。也就是说，该图像由图像视野公共和非公开信息组成。用来重建原始3D模型的最重要的信息可以被描述为和，其中，。和分别是两台CCD图像中的点数。然而，其他的点，例如和，找不到在照相机平面上的对应点。

为了提取从两个摄像头图像的公共信息，我们也建立像其他论文一样整流过的照相机平面。这个平面参照了两个图像的公共线路和基线。根据相似原理和平行四边形的理论，在整流平面结构保持一致时物体的世界点与参照经整流的平面也就是匹配平面在同一平面上。即，两个映射结构可以在匹配平面中匹配良好。

## 4.1基于整流坐标重建算法

颗粒图像是由上述的整流系统（在图5中示出）进行处理。A和B是在匹配平面中的随机点。 P和Q分别是两个摄像机的光学中心。 C，D，E和F是A和B的投影。

在整流系统中，我们定义了3D参数：P(a,b,c), Q(e,f,g), E(x2,y2,z2), C(x1,y1,z1) 和|PQ| = B， |CE| = d和 Eq. (2) 可以从相似原理导出。

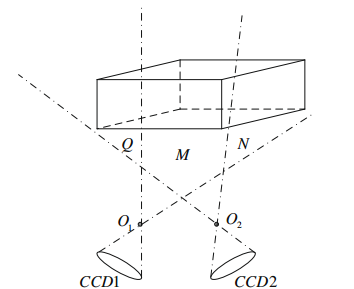


图4.两个CCD相机不同角度的照片模型

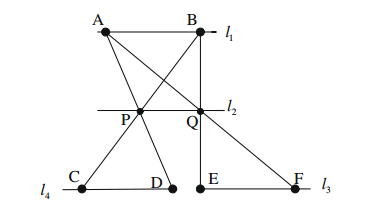
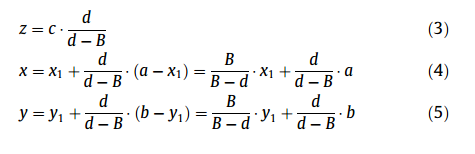


图5.双眼视觉的几何描述



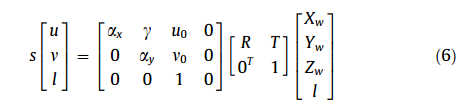
根据平行投影的原理，我们可以获得：, , , f = b, c = g, e = a + B.下面结论可由公式（2）得出



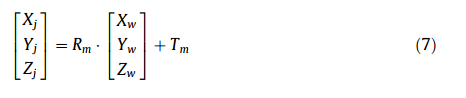
由公式（3）-（5），我们可以清楚地得到了在世界体系中的目标位置依赖于大量的差别信息。使用公式（3），公式（4）和公式（5），能够得到在整流系统中的对象的坐标。然后，我们就可以获得根据投影关系的世界坐标。

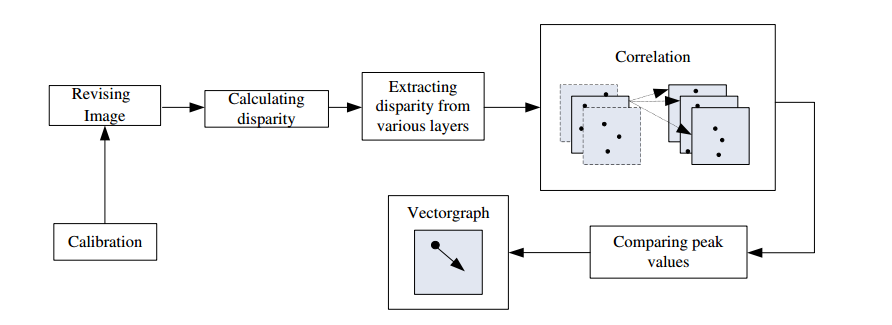
## 4.2基于双目视觉分析流场内任意点

和其他的视觉测量系统一样，测量前需要标定[11–16]。图像坐标之间的关系 （，）和世界坐标（，，）由公式（6）给出。

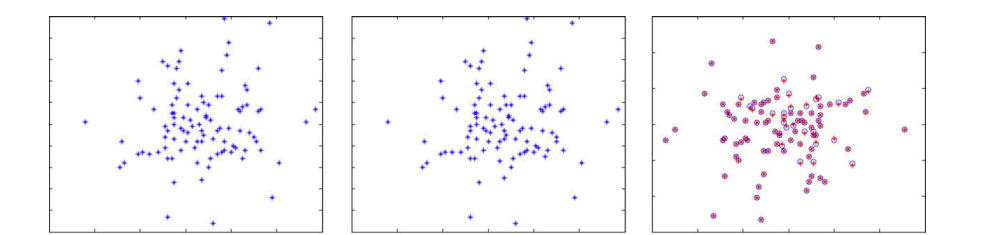


其中，s为任意比例因子；和分别是水平和垂直方向的焦距；（）是基准点的坐标，是光轴与视网膜平面的交点；是非正交轴模型的歪斜因数；R和T分别是旋转矩阵和平移矩阵。同时，根据公式（7）所示的坐标转化原理，我们可以得到整流系统与世界系统的坐标关系。





图六. 基于双目视觉粒子图像测速系统

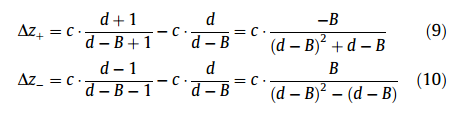


（a）左相机粒子图像 （b）右相机粒子图像 （c）整流匹配粒子

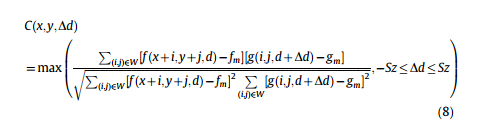
图7. 空间平面整流匹配。（（c）中的蓝色圆圈代表左相机的校正平面，红色圆圈表示右相机的校正平面。）（对于这个图例中提及的颜色解释，读者可以参考本文的网络版本。)

其中，和是校正坐标；，和是世界坐标。和分别是旋转矩阵和平移矩阵。

不同坐标之间的关系需要标定之后确定。然后，我们需要提取来自两个CCD图像平面的有用信息。如前面提到的，在相同的匹配平面上的点的结构和整流后是相同的。因此，通过视差修正的图像可匹配其公共信息可被提取。有视差信息的图像可以用于重建三维模型。这一过程会一直重复，直到所有的点都进行了分析。所提取的图像，（1,2,3，...，）包括视差信息。用同样的方法在一个时间间隔后来提取视差图像即，（1,2,3，...，）。给一个世界系统的坐标点，我们能通过公式（3）-（7）得到整流系统中相应的坐标点。首先，建立一个以中的分析点为中心的审讯窗口。然后，在相应窗口内的数据被选择和处理。在本文中，我们采用的PTV方法处理稀疏分布的颗粒[17-19]，并采用互相关方法来处理密集分布的颗粒[20-22]。视差相关修改被下面显示，其中所述询问窗口的大小与被测流体的最大速度相关，并且通常符合“1/4原则”。沿Z方向的视差的变化可以描述如下：



根据公式（8），选择每一层最大位置作为粒子运动的新位置。除以一帧和下一帧之间两个位置的间隔距离，那么我们就可以得到该点的测速。该过程如图6所示：首先，标定相机；第二，校正图像；第三，选择匹配的平面；最后，关联颗粒图像，并计算运动矢量。



# 5.结果与讨论

为了测试在3DPIVS双眼视模型的性能，已经完成一些实验其中包括合成实验和实际的实验。在模拟实验中，前面提到的，颗粒被假设为服从高斯分布，符合在实际中分散的规则。

## 5.1空域整流实验

为了验证该整流能力，具有高斯分布的颗粒被用于整流和匹配。首先，我们提取匹配平面不同的空间层次。然后，视差被消除。图7给出了100点在平面Z= 20的处理结果。图7（a）和（b）分别描绘左相机和右相机的粒子图像。图7（c）是消除视差整流一体化的粒子图像。从结果来看，我们可以清楚地看到粒子，在整流平面左，右相机中彼此对应。表1所示出几个实验的匹配误差平均值。

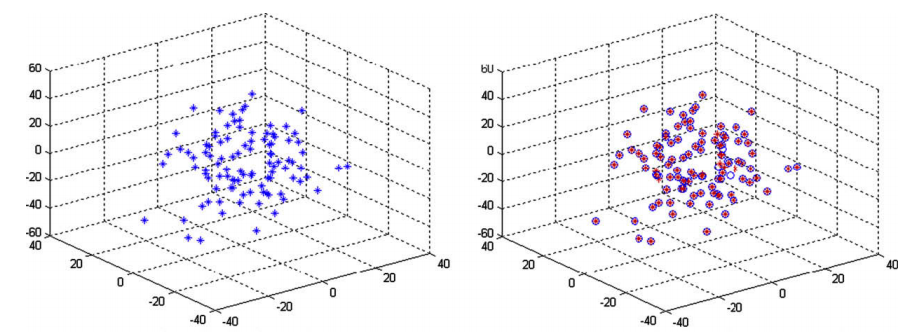
**表1**

校正图像的匹配误差

|  |  |  |
| --- | --- | --- |
| 目标 | U | V |
| 平均匹配误差（mm） | 0.48 | 0.49 |

## 5.2空间片段提取和重建

在实验中，我们预测图像平面的空间点。然后该图像被整流和颗粒的空间片段被提取。粒子图像的空间计算在获得的视差图之后被提取。最后，经整流的坐标被转换为世界坐标。因此，颗粒的重建完成。在此过程中的点的数量为50-100000。空间区域是：X：从-200至200，Y：从-200至200中，Z：从-50到50。图8所示，100个空间点的三维图像和校正重建后的匹配图像。我们可以看到，93％的空间点正确重建。

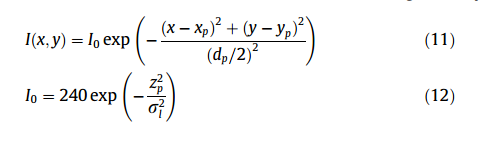


（a）100个高斯分布的粒子 （b）空间粒子重建

图8. 空间粒子重建（（b）中红色代表原来的空间点，蓝色代表的重建结果）（对于本图例中提及的颜色解释，读者可以参考本文的Web版本）

## 5.3 3DPIVS模拟实验

为了验证3DPIVS的算法，几个粒子图像根据流体流动的特征合成。图9显示代表性的结果（=5.0，=500.0）。在实验的图像，256强度级（8位）被定义和图像中的位置（x，y）的强度因粒子（，）散射影响被表示为[23]：

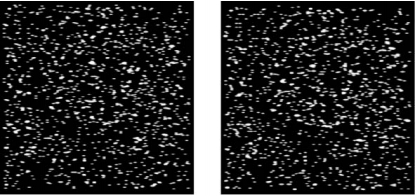


其中是激光光片的厚度;（，，）是粒子的位置；是颗粒的大小。粒子的速度被表示为= +2x， = z +2x，= x +2y。在图6中所示的方法被用来在图像处理期间，计算颗粒图像。首先，获得整流粒子分布（图10），并使用由层提取信息校正粒子图像。然后，计算出的一帧和下一帧之间的位移。最后，重建世界坐标和得到在图11中所示的空间矢量场。（为了清楚地显示该矢量场，在此过程中产生的空白区域被通过内插法修正，并由流动方程限制。）表2表示误差，从表2和图11，我们可以看到，双目PIV模型能更准确地提取三维流场信息。

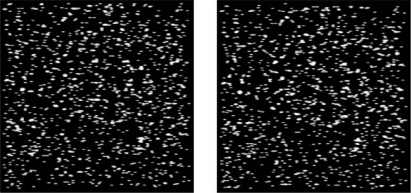
**表2**

双眼PIV模型误差

|  |  |  |  |
| --- | --- | --- | --- |
| 目标 | X | Y | Z |
| 平均误差（%） | 6.3 | 5.9 | 11.4 |

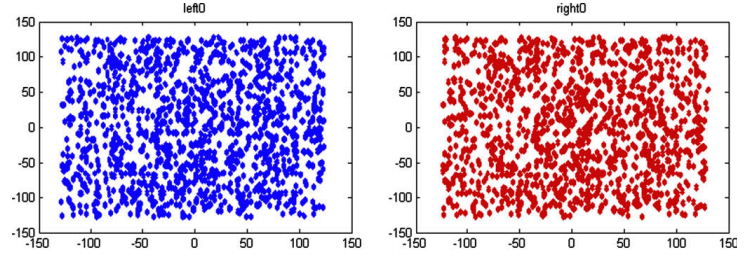


（a）t时间左图像 （b）t时间右图像



（c）t+ （d）t+时间右图像

图9. 合成的粒子图像



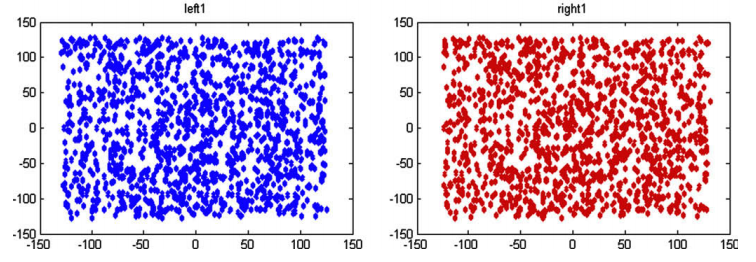


图10. 整流平面颗粒分布

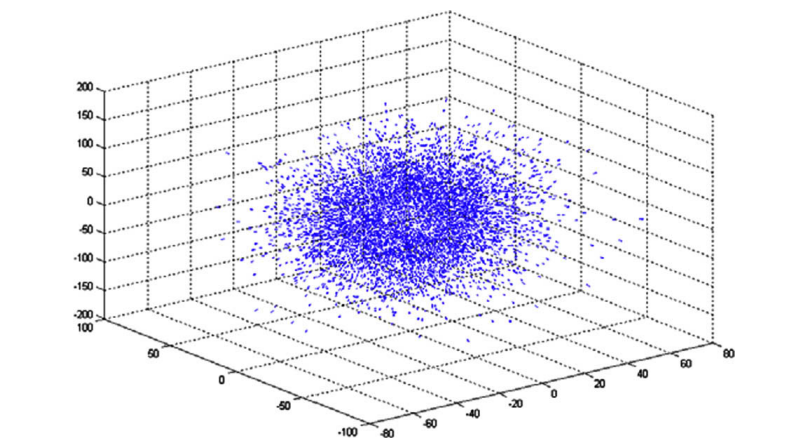


图11. 插值与拟合后的粒子的空间矢量

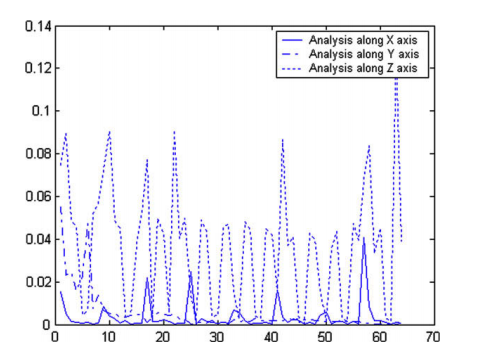
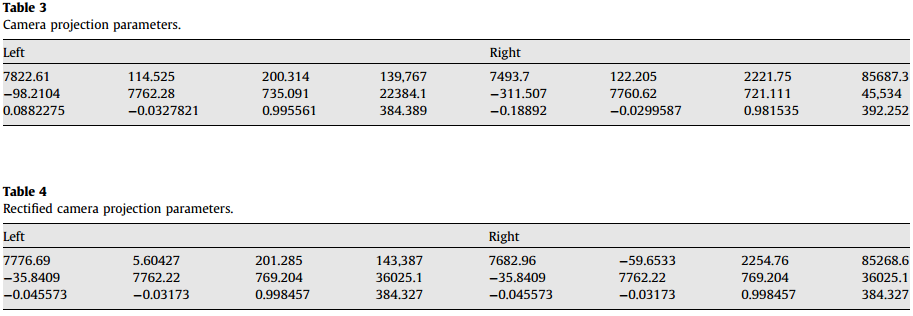


图12. 三维重建中的误差

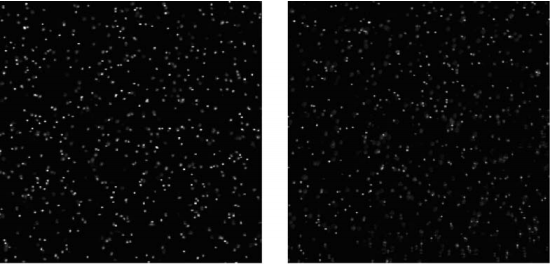
## 5.4真正的流体流动分析

为了评估在本文提出的3DPIVS方法的性能，我们使用两个CCD相机来分析在水槽的流场。在实验过程中，两个摄像机（IPX-2M30L由Imperx的生产）用相同的模型被置于水槽的一边，两个照相机的光轴是同一个固定的角度。大约5厘米厚的水从下方照亮。流体流动被直径为150的聚苯乙烯泡沫塑料颗粒可视化。图像收集后系统被调整，CCD相机需要校准。为方便起见，我们得到了实验地方（在表3中示出）的投影矩阵。同模拟实验不同，在实践中，两个摄像机不能放置成彼此平行。所以，我们必须在处理前转化表3和表4中的投影矩阵。

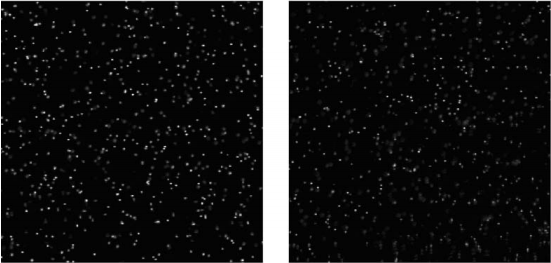
图12描述了三维重建的性能。图12中，64点并不是在校准板的中心区域而是被随机地选择并进行计算。图12显示出了沿Z轴的误差比沿X轴和Y轴（其中，沿X轴和Y轴误差都低于0.06）大。平均误差小于0.13，是可以接受的。



校准后，PIV实验开始。图13中示出的粒子图像是从不同的CCD相机在不同的时间获得的。（为了清楚地表明，我们削减了图像尺寸1200\*160到256\*256）。图14（a）和（b）分别示第200行到第455行中的整流平面矢量场的左视图和右视图。（审讯窗口在匹配过程中只研究一个与整流平面平行的分割面。）分析的尺寸是16\*16，大部分区域可以实现提取动向量。1664区域中1330进行了分析。也就是说，约80％的点进行了分析。图15示出重建的结果。图15（b）示出了局部放大结果。从实验结果中，我们可以看到，一定量的矢量场可以通过该算法被提取。结果符合实际运动和最近向量是相似的和连续的。所以这样的结果是有效的。



（a）左相机第一帧 （b）右相机第一帧



(c)左相机第二帧 (d)右相机第二帧

图13.真实粒子图像

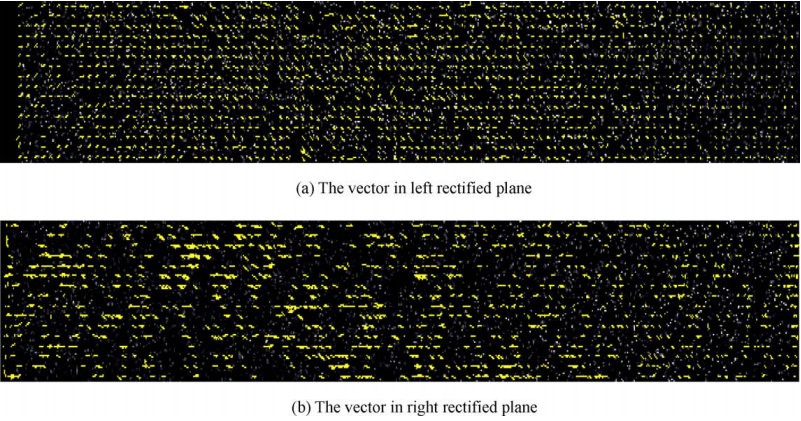
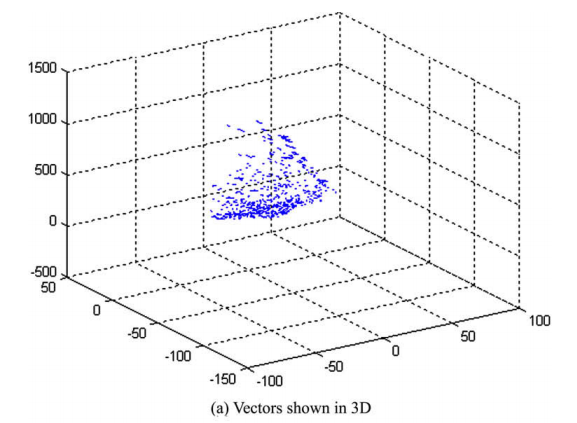


图14. 颗粒图像的处理结果



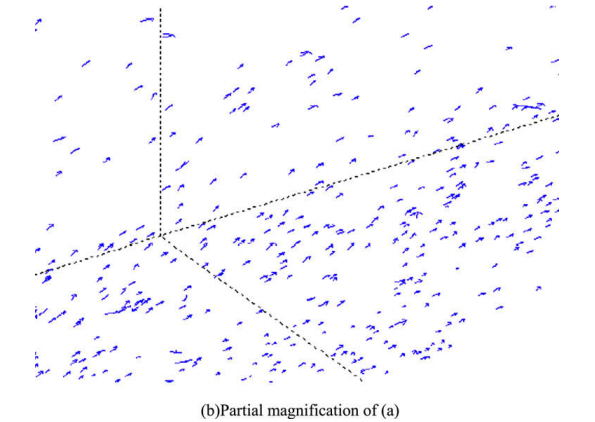


图15.矢量场三维重建

# 6.结论

用于颗粒图像匹配和重建的一般立体视觉方法仅当颗粒分布非常稀疏，激光切片较薄时使用。它不适和在大规模空间计算微粒速度。在本文中，我们在立体计算的基础上建立3DPIVS模型，提出了一种基于层的相关性和提取方法。该方案可以克服在立体匹配和空间信息表达上的困难。也就是说，首先处理所述三维粒子空间层按层和提取的所需平面。然后由PIV或PTV方法计算粒子场的运动，方法由询问窗口颗粒的特征所确定。该3DPIVS模型可以整齐地和准确地提取空间层，并且可以进行精确的空间匹配。最后，校正平面实验，空间切片重构实验，合成粒子图像的实验和实际的流体流动实验都表明，该模型是可靠的，矢量场中任意点可以准确地计算出来。

7.参考

[1] R.J. Adiran, Particle imaging techniques for experimental fluid mechanics, Annu. Rev. Fluid Mech. 23 (1991) 261–304.  
[2] S.K. Prasad, R.J. Adrian, Stereoscopic particle image velocimetry applied to liquid flows, Exp. Fluids 15 (1993) 49–60.  
[3] E.P. Fabry, 3D holographic PIV with a forward-scattering laser sheet and stereoscopic analysis, Exp. Fluids 24 (1998) 39–46.  
[4] H.Q. Sun, H.G. Kang, Processing of DPIV data, J. Dalian Univ. Technol. 40 (3) (2000) 364–367.  
[5] S. Ansoldi, G.B. Buora, V. Roberto, 3D reconstruction as a network service, Proc. Int. IEEE Conf. Comput. Archit. Mach. Percept. 6 (2005) 294–299.  
[6] D. Huber, O. Carmichael, M. Hebert, 3-D map reconstruction from range data, Proc. Int. IEEE Conf. Robot. Automat. (2000) 891–897.  
[7] N.D.B. Bruce, J.K. Tsotsos, An attentional framework for stereo vision, Proc. Int. IEEE Conf. Comput. Robot. Vis. 9 (2005) 88–95.  
[8] Y.Z. Wang, D.S. Li, C. Liu, A stereoscopic imaging model and its calibration of micro stereovision for 3D measurement, Proc. Int. IEEE Conf. Info. Acquisition 27 (2005) 6.  
[9] C.L. Zitnick, T. Kanade, A cooperative algorithm for stereo matching and occlusion detection, IEEE Trans. Pattern Anal. Mach. Intell. 7 (22) (2000) 675–684.  
[10] W.S. Kim, A.I. Ansar, R.D. Steele, R.C. Steinke, Performance analysis and validation of a stereo vision system, Proc. Int. IEEE Conf. Syst. Man Cybern. 2 (2005) 1409–1416.  
[11] R.Y. Tsai, A versatile camera calibration technique for high-accuracy 3D machine vision metrology using off-the-shelf TV camera and lenses, IEEE J. Robot. Automat. 3 (4) (1987) 323–344.  
[12] A. Isaguirre, P. Pu, J. Summers, A new development in camera calibration calibrating a pair of mobile cameras, Proc. Int. IEEE Conf. Robot. Automat. (1985) 74–79.  
[13] O.D. Faugeras, G. Toscani, Calibration problem for stereo, Proc. Int. Conf. Comput. Vis. Pattern Recognit. (1986) 15–20.  
[14] R.K. Lenz, R.Y. Tsai, Techniques for calibration of the scale factor and image center for high accuracy 3D machine vision metrology, Proc. IEEE Int. Conf. Robot. Automat. (1987) 68–75.  
[15] R.Y. Tsai, A versatile camera calibration technique for high-accuracy 3D machine vision metrology using off-the shelf TV cameras and tenses, IEEE J. Robot. Automat. 4 (3) (1987) 323–344.  
[16] J. Weng, P. Cohen, M. Herniou, Camera calibration with distortion models and accuracy evaluation, IEEE Trans. Pattern Anal. Mach. Intell. 10 (14) (1992) 965–980.  
[17] K. Okamoto, W.D. Schmidl, Y.A. Hassan, Least force technique for the particle tracking algorithm, Proc. 1st Int. (1995) 21.  
[18] K. Nishino, K. Torii, A fluid-dynamically optimum particle tracking method for 2D PTV: triple pattern matching algorithm, Transport Phenom. Therm. Eng. (1989) 1411–1416.  
[19] L. Zimmer, J.M. Buchlin, M.L. Riethmuller, Particle tracking velocimetry and sizing: application to liquid sprays, Proc. Int. Part. Image Velocimetry (1999) 16–18.  
[20] F. Yamamoto, A. Wada, M. Iguchi, M. Ishikawa, Discussion of the cross-correlation methods for PIV, J. Flow Vis. Image Process. 3 (1996) 65–78.  
[21] M. Ishikawa, F. Yamamoto, Y. Murai, M. Iguchi, A. Wada, A novel PIV algorithm using velocity gradient tensor, Proc. Int. PIV (1997) 51–56.  
[22] A. Stitou, M.L. Riethmuller, Extension of PIV to super resolution using PTV, Meas. Sci. Technol. 12 (2001) 1398–1403.  
[23] K. Okamoto, S. Nishio, T. Saga, et al, Standard images for particleimage velocimetry, Meas. Sci. Technol. 11 (6) (2000) 685–691.