文章编号:1001 - 9081(2007)05 - 1067 - 03

一种基于 FastICA 的图像隐写提取算法

李祁云[1],李建平[2,3],肖书成[2]
(1. 解放军后勤工程学院 研究生四队,重庆 400016;
2. 解放军后勤工程学院 国际小波分析应用研究中心,重庆 400016;
3. 电子科技大学 计算机科学与工程学院,四川 成都 610054)
(lqyxyww@126.com)

摘 要:针对隐写术的特点,提出了一种新的隐写提取算法。该算法不同于传统提取算法基于逆嵌入算法的思想,将快速独立分量分析(FastICA)引入提取算法中,进行载体图像与秘密图像的分离。隐写是在真彩色图像的小波系数上进行的,有效地将近几年来比较热门的隐写术、小波分析与独立分量分析结合在一起。实验验证独立分量分析技术不仅能够用于秘密信息提取而且还能够实现真正的盲提取。

关键词:隐写术;快速独立分量分析;小波系数;阈值
中图分类号: TP309.2 **文献标识码**:A

New extraction method of image steganography based on FastICA

LI Qi-yun[1], LI Jian-ping[2,3], XIAO Shu-cheng[2]
(1. *Unit 4 of Postgraduate Department, Logistical Engineering University, Chongqing* 400016, *China*;
2. *International Centre for Wavelet Analysis and Applications, Logistical Engineering University, Chongqing* 400016, *China*;
3. *School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan* 610054, *China*)

Abstract: According to the features of steganography, a new extraction was proposed. Different from the traditional extraction based on the invert embedding, this new extraction used FastICA to separate the cover image and embedded image. The objects which have been treated with were wavelet coefficients of true color picture, so steganography, wavelet and Independent Component Analysis (ICA) were combined together. The effect of algorithm proves that ICA can not only be used as extraction but also extract the embedded image blindly.

Key words: steganography; Fast Independent Component Analysis(FastICA); wavelet coefficients; threshold

0 引言

随着信息安全技术的不断发展和丰富,信息隐藏技术作为信息安全中的一项重要技术,近十年来引起了国内外学术界和相关部门的重视。隐写术作为信息隐藏技术中最为重要的两个分支之一,近年来受到了广泛的关注。隐写术(Steganography)这个词语本身的意思是“掩饰性地写”,通常被解释为将秘密信息隐藏在其他信息中。它以图像、音频等数字媒体作为掩护,把要发送的秘密消息嵌入到载体信号内部,以不引起外界注意的方式通过公共信道,特别是互联网进行传递。它与水印同属信息隐藏范畴,有许多共性但也存在着差异,如通信内容不同:水印的通信内容是宿主信号本身,而隐写的通信内容是被隐蔽的消息;鲁棒性要求不同:水印必须高度鲁棒,而隐写则不要求很强的鲁棒性,因为它通常应用于无扰信道等等。

图像隐写包括嵌入算法和提取算法两个部分,简单地说嵌入算法就是将载体图像与秘密图像进行混合,而提取算法则是让载体图像与秘密图像分离,使得秘密信息尽可能完整地从混合图像中提出。提取秘密信息以往惯用的方法就是将提取算法作为嵌入算法的逆算法,怎么嵌入秘密信息就怎么用逆方法进行提取;或者是使用原始载体图片来得到秘密信息。本文考虑到独立分量分析(ICA)是一种将信号分解成若干个互相独立成分的信号处理方法,它能够有效地将混合信号进行分离,所以将其引入了提取算法中。

目前,已有一些研究人员将独立分量分析引入了信息隐藏领域,但大多存在于数字水印方面,用于隐写术的文章很少。目前,将 ICA 引入数字水印的文章主要分为两类,第一类是在水印嵌入时就将 ICA 引入了,而非单纯地用于提取[1]。第二类则仅在水印检测、提取时使用 ICA,如文献[2,3]就是将载体图像和水印线性变换后得到的数据作为第一条观测信号,再利用原始图像的信息组成第二条或第三条观测信息,进行 ICA 提取。同样的方法也在文献[4]中出现了,只不过该论文将第二条观测信号进行了加密。这些文章在提取时基本上都使用了原载体图片信息,没有实现真正意义上的盲提取,这在使用中受到一定的限制,而且存在无法说明被提取水印来源的问题。文献[5,6]则提出将原始图像和水印图像在嵌入前就进行混合,取其中一条混合信号进行嵌入操作,另一条作为密钥,提取时利用这两条混合信号进行 ICA。虽然此方

收稿日期:2006 - 11 - 27;**修订日期**:2007 - 02 - 05

作者简介:李祁云(1982 -),女,湖南永州人,硕士研究生,主要研究方向:信息隐藏; 李建平(1964 -),男,湖南祁阳人,教授,博士生导师,主要研究方向:小波分析、信息安全; 肖书成(1975 -),男,重庆人,讲师,硕士研究生,主要方向:网络安全.

法未用到载体图像的信息,但需要另外负载一大串的密钥以便进行提取。

基于隐写术与水印的不同点,本文提出一种专适用于隐写术的 ICA 提取算法。对于嵌入算法,可引用其他文章提出的嵌入方法,无须做任何特别的更改,我们所需做的仅仅是进行两次嵌入操作而已;对于提取算法,快速 ICA(FastICA)被引入了进来,提取过程中无需载体图片的信息,仅仅需要提取密钥(阈值)即可提取秘密信息,方便简单,实现了秘密信息的真正盲提取。

1 独立分量分析

独立分量分析是信号处理领域在 20 世纪 90 年代后期发展起来的一项全新的信号处理和数据分析方法。顾名思义,它的含义是把信号分解成若干个互相独立的成分。图 1 是 ICA 最简单的框图说明。多导观察 $\boldsymbol{X}$ 是多个信源 $\boldsymbol{S}$ 经混合矩阵 $\boldsymbol{A}$ 组合而成($\boldsymbol{X}=\boldsymbol{A}\boldsymbol{S}$)。现在的任务是:在 $\boldsymbol{S}$ 与 $\boldsymbol{A}$ 均为未知的条件下,求取一个解混矩阵 $\boldsymbol{B}$,使得 $\boldsymbol{X}$ 通过它后所得输出 $\boldsymbol{Y}$($\boldsymbol{Y}=\boldsymbol{B}\boldsymbol{X}$)是 $\boldsymbol{S}$ 的最优逼迫。独立分量分析实际上是一个优化问题,因为问题没有唯一解,只能在某一衡量独立性的判据最优的意义下寻求其近似解答,使 $\boldsymbol{Y}$ 中各分量尽可能相互独立;$\boldsymbol{Y}$ 与 $\boldsymbol{S}$ 不但只是近似,而且在排列次序和幅度上都允许不同。

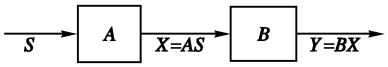


图 1 ICA 的简单框图说明

1.1 ICA 的数学模型

ICA 问题的混合—解混过程如图 2 所示,其中解混系统 $\boldsymbol{B}$ 就是 ICA 过程。

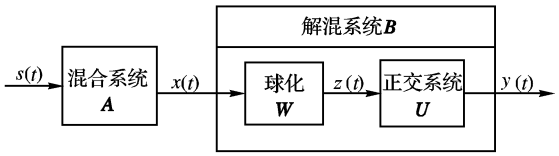


图 2 混合—解混过程简图

假设混叠系统有 m 个传感器和 n 个源信号,源信号与观察信号之间的关系如下:

$$\boldsymbol{X}(t)=\boldsymbol{A}\,\boldsymbol{S}(t)$$

其中观察信号 $\boldsymbol{X}(t)=\left[x_1(t),x_2(t),\cdots,x_m(t)\right]^{\mathrm{T}}$ 是 m 个未知的源信号的混叠,而且 n 个源信号

$\boldsymbol{S}(t)=[s_1(t),s_2(t),\cdots,s_n(t)]^{\mathrm{T}}$,$s_i(t),i=1,2,\cdots,n$ 是相互统计独立的。混叠矩阵

$\boldsymbol{A}=(a_{ij}),i=1,2,\cdots,m;j=1,2,\cdots,n$

是一个 $m\times n$ 阶的矩阵。

盲源分离就是求解矩阵 $\boldsymbol{B}$,使得通过下面的公式可以恢复得到源信号 $\boldsymbol{S}(t)$:

$$\boldsymbol{Y}(t)=\boldsymbol{B}\,\boldsymbol{X}(t)=\hat{\boldsymbol{S}}(t)$$

在没有关于混叠矩阵 $\boldsymbol{A}$ 和源信号 $\boldsymbol{S}(t)$ 的任何先验信息的情况下该问题是没有解的。因此通常认为:(1) 源信号 $s_i(t),i=1,2,\cdots,n$ 是平稳的随机信号,且是相互统计独立的;(2) $\boldsymbol{A}$ 是满秩的,一般设 $m=n$;(3) 至多一个源信号为高斯的。这样利用源信号统计独立的假设,可以恢复出源信号[5]。

目前,对于分离矩阵 $\boldsymbol{B}$ 的求解方法很多,本文选用 Aapo Hyvarinen 等人提出的“快速 ICA 算法”来进行提取。

1.2 快速 ICA 算法

1997 年芬兰学者 Aapo Hyvarinen 等人首先提出基于四阶累计量的固定点算法。其后,在 1999 年又提出了进一步的改进——基于负熵的 ICA 固定点算法。在 2001 年出版的著作中他们又作了进一步简化。由于这一算法比批处理甚至自适应处理,具有更快的收敛速度,因此又被称为”快速 ICA 算法”。

多个独立分量逐次提取的 FastICA 算法步骤如下[7]:

(1) 把原始数据 x 去均值,再球化,得 z;

(2) 设 m 为待提取独立分量的数目,令 $p=1$;

(3) 任意取 $u_p(0)$,但要求 $\left\|u_p(0)\right\|_2=1$;

(4) 迭代:

$$u_p(k+1)=E\left\{zf\left[u_p^{\mathrm{T}}\left((k)z\right)\right]\right\}-E\left\{f'\left[u_p^{\mathrm{T}}(k)z\right]u_p(k)\right\}$$

f,f' 可见表 1,总集均值用时间均值代替。

表 1 $F(\cdot)$,$f(\cdot)$ 与 $f'(\cdot)$

$F(y)$	$f(y)$	$f'(y)$
$\frac{1}{a_1}\log\cosh a_1 y$	$\tanh a_1 y$	$a_1[1-\tanh^2(a_1 y)]$
$-e^{-\frac{y^2}{2}}$	$ye^{-\frac{y^2}{2}}$	$(1-y^2)e^{-\frac{y^2}{2}}$
y^4	y^3	$3y^2$

(5) 正交化:$u_p(k+1)-\sum_{j=1}^{p-1}[u_p(k+1),u_j]u_j\rightarrow u_p(k+1)$

(6) 归一化:$\frac{u_i(k+1)}{\|u_i(k+1)\|_2}\rightarrow u_i(k+1)$

(7) 如 u_p 未收敛,回到步骤(4);

(8) 令 p 加 1,如 $p\leqslant m$,则回到步骤(3)。否则工作完成;

注意:式中 k 是迭代序号,不是时间序号。$E(\cdot)$ 可以通过对 z 的各采样时刻值求均值来估计。

2 基于 FastICA 的隐写提取算法

为确保 ICA 模型的可识别性,要求线性混合的观测信号数目至少等于或大于独立源的数目。对于本文的提取算法,需要进行两个独立分量的提取,所以至少要求有两个观测信号,而在仅有隐藏图像,无载体图像的情况下,只能得到一个观测信号。为得到两条观测信号,我们实施了两次嵌入算法。所以本文选用真彩色图像作为载体对象。原因是:1) 由于真彩色图像具有红、绿、蓝三个分量矩阵,我们可以分别在各颜色分量上进行嵌入。考虑到人眼对颜色的敏感程度,我们选择在红色和蓝色分量上分别进行一次嵌入。2) 真彩色图片很普遍,如从数码相机中,从网络上都很容易得到。嵌入算法与提取算法构成了隐写的整体,两者联系紧密,为了使提取算法容易理解,作为提取算法的铺垫,我们须介绍嵌入算法。

2.1 嵌入算法

在本论文里,我们将希望被秘密保存的信息称为嵌入对象,将用于隐蔽嵌入对象的非保密载体称为掩体对象。嵌入对象通过嵌入过程被隐藏在称为掩体对象的非保密信息中,从而生成隐藏对象。下面是具体的嵌入步骤:

1) 由于本文考虑的隐写是在频域嵌入法中的小波系数上进行的,所以首先对嵌入对象进行小波分解,得到小波系数矩阵 $\boldsymbol{V}$。

2）对掩体对象的红色矩阵进行小波分解,得到系数矩阵 M。由嵌入人员取定一个阈值(作为提取密钥)。将大于阈值的系数存于矩阵 W 中,这些系数在 M 中的坐标存于数组 S 中,将 V 中的系数与 W 中的系数相加,根据 S 修改 M 中的原系数值。再对系数矩阵 M 进行小波重构,即可得到隐藏对象的红色矩阵。再将 V 中的系数与 W 中的系数进行线形变换,即

$$P = \alpha V + \beta W$$

这里我们取 $\alpha = 0.1, \beta = 0.2$,可得到系数矩阵 P。

3）对掩体对象的蓝色矩阵进行小波分解,得到系数矩阵 N。根据数组 S,用 P 中的值依次替换 N 中的原始系数。即可得到加载了秘密信息的另一副小波系数。对系数矩阵 N 进行小波重构,嵌入算法完成。

2.2　提取算法

隐写与水印一个很大的不同在于:水印的载体信息在水印提取后仍然具有商业价值,而隐写术中的载体信息扮演的唯一角色是掩盖通信的存在,掩体对象的内容对发送者和接收者来说没有价值[8],所以在提取时完全可以将掩体对象当作噪声来剔除掉,因此在提取算法中我们只注重嵌入对象的系数,ICA 中所需要的观测信号的长度只需跟嵌入对象的系数长度一样就行了。具体的提取算法步骤如下:

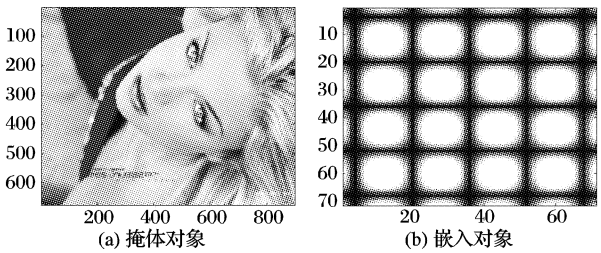
(1) 对隐藏对象的红色矩阵进行小波分解,得到系数矩阵 C。将大于密钥阈值的系数存于一维数组 A 中作为第一条观测信号,将这些系数在 C 中的坐标存于数组 S 中。

(2) 对隐藏对象的蓝色矩阵进行小波分解,得到系数矩阵 W。依据数组 S,从 W 中寻找出相应的系数值,存入一维数组 B 中作为第二条观测信号。

(3) 用(1) 中的数组 A 和(2) 中的数组 B 组成两条观测信号,应用 FastICA 进行分离,可得到掩体对象的部分小波系数和嵌入对象的全体系数,进行小波重构,可得嵌入对象。

3　实验

这一节我们将对 FastICA 的提取效果进行验证,选择下面两幅图作为掩体对象和嵌入对象,见图 3。



(a) 掩体对象　　(b) 嵌入对象

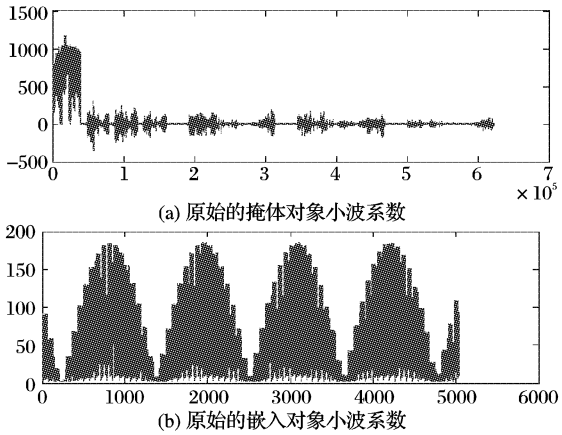
图 3　掩体对象和嵌入对象

图 3 中掩体对象与嵌入对象的小波系数图如图 4,对隐藏对象进行 FastICA 后得到的掩体对象和嵌入对象的小波系数图如图 5 所示。

结论:

(1) 从图 4 和图 5 可以看出,图 4 中的嵌入对象系数图与图 5 中的嵌入对象系数图形状上非常相似,几乎一模一样,不同的地方在于图 5 中的那幅图幅值范围要小得多,只位于 $-1 \sim 3$ 之间,而图 4 中的幅值位于 $0 \sim 200$ 之间,这都是 FastICA 预处理球化造成的结果。我们可以通过调整幅值的范围,将两幅图更加的接近,以进行提取。

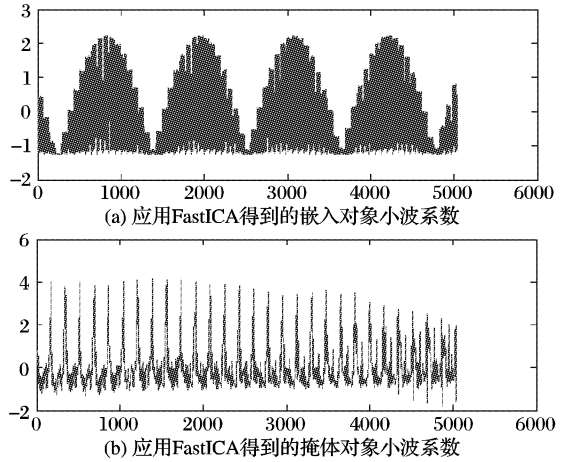
(2) 从图 4 和 5 还可以看出,嵌入对象的小波系数图在两幅图中出现的位置是不同的,这正好说明了 ICA 提取的顺序不确定性,这也是为什么我们要进行两次提取的原因。因为不能够确定进行一次提取后提取出来的是嵌入对象的系数。



(a) 原始的掩体对象小波系数

(b) 原始的嵌入对象小波系数

图 4　原始的掩体对象小波系数和嵌入对象小波系数

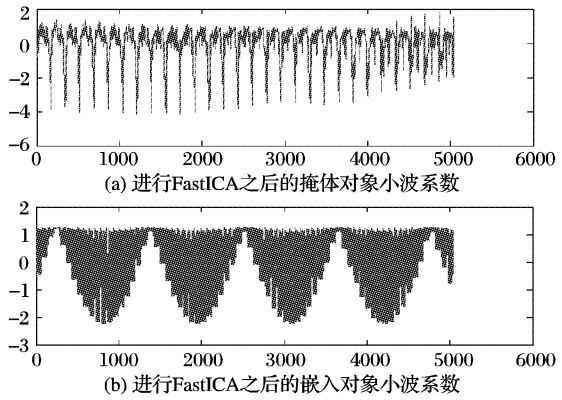


(a) 应用FastICA得到的嵌入对象小波系数

(b) 应用FastICA得到的掩体对象小波系数

图 5　应用 FastICA 得到的嵌入对象小波系数和掩体对象小波系数

由于 ICA 还允许在幅度上不同,所以有可能得到幅值相反的图像,如图 6。



(a) 进行FastICA之后的掩体对象小波系数

(b) 进行FastICA之后的嵌入对象小波系数

图 6　进行 FastICA 之后的掩体对象小波系数和嵌入对象小波系数

图 5(a) 与图 6(b) 形状上是一样的,只是幅值正好方向相反,如果出现图 6 的结果可以多运算几次,便可得到图 5(a) 的图形。

将得到的小波系数进行重构,得结果如图 7。

由图 7 可以看出,嵌入对象被成功提出,即为图 7(a),图 7(b) 为一幅伪乱码,原因是我们在取观测信号时,未把掩体对象的全部系数取入,而是只取了负载秘密信息的那部分

(下转第 1076 页)

从图5、图6可以看出，MBCR由于选择的是能源较大的路径，所以，它的丢包率和网络生存时间都较好；DSR协议没有考虑能源问题，在这方面的性能最差，而BEOP协议与MBCR协议较接近。

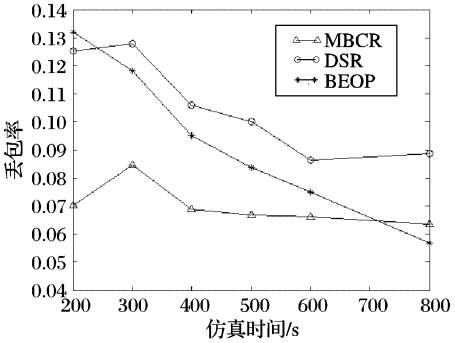


图5 丢包率变化情况

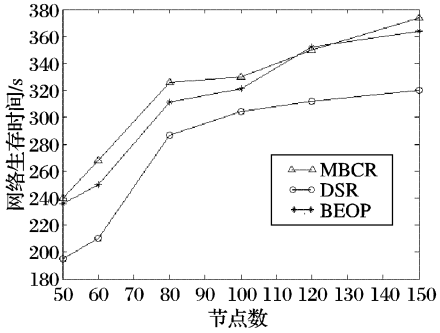


图6 网络生存时间

5 结语

本文提出了一种节点平衡估价函数BEF，该函数利用了节点的历史信息，通过它能够找到网络中有较好性能的节点。基于节点的平衡估价函数提出了一种新的路由协议BEOP，该协议能够使得多种网络性能参数都达到一个较好的指标。与DSR和MBCR协议比较，该协议在网络的平均时延、吞吐量、控制开销、丢包率、包成功发送率及网络生存时间等性能上都有较好的改善。下一步的研究工作主要包括进一步优化平衡估价函数，并将之应用到组播路由中。

参考文献：

[1] MACKER J, CORSONS. Mobile Ad Hoc networks (MANET) [EB/OL]. http://www.ietf.org/html.charters/manet-charter.html, 1997-10-10.

[2] PERKINS CE, BHAGWAT P. Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers [A]. Proceedings of ACM SIGCOMM'94[C]. 1994. 234-244.

[3] PERKINS CE, ROYER EM, DAS SR. Ad Hoc On-Demand Distance Vector(AODV) Routing[EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-13.txt, 2003-10-10.

[4] JOHNSON DB, MALTA DA, YIH-CHUN HU. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks[EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt, 2003-10-10.

[5] HAAS ZJ, PEARLMAN MR, SAMAR P. The Zone Routing Protocol for Ad Hoc Networks[EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-manet-zrp-04.txt, 2002-10-10.

[6] JACQUET P, MUHLETHALER P, QAYYUM A. Optimized Link State Routing Protocol [EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-manet-olsr-00.txt, 1998-10-10.

[7] JIANG ML, LI JY, TAY YC. Cluster Based Routing Protocol (CBRP)[EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-manet-cbrp-01.txt, 1999-10-10.

[8] SINGH S, WOO M, RAGHAVENDRA CS. Power Aware Routing in Mobile Ad Hoc Networks[A]. Proceedings of Mobicom'98 Conference[C]. 1998.181-190.

[9] SCOTT K, BAMBOS N. Routing and Channel Assignment for Low Power Transmission in PCS[A]. ICUPC'96[C]. 1996.498-502.

[10] TOH CK. Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks[J]. IEEE Communications Magazine, 2001,(6):138-147.

(上接第1069页)

系数，所以经ICA后得到的掩体对象系数的数量是不足以进行掩体对象还原的。

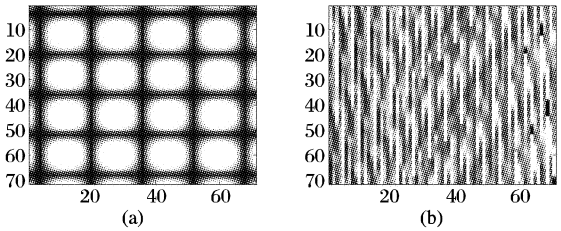


图7 经ICA提取后得到的图像

4 结语

基于ICA的作用，本文提出一种新的隐写提取算法，该算法的使用前提是在掩体对象中进行两次隐写嵌入，以确保ICA模型的可识别性。本算法在提取时只需要一个密钥，就可得到观测信号，利用观测信号，不需要掩体对象、嵌入对象等其他信息，便能有效地提取嵌入对象，随后的实验也验证了该算法的提取效果。提取过程中为得到两条观测信号，本文使用了真彩色图像作为掩体对象。怎样将该算法应用于任意类型的掩体对象，以及如何进行两次嵌入后隐蔽性达到最高是即将要研究的问题。

参考文献：

[1] 刘琚，孙建德. 基于图像独立特征分解的数字水印方法[J]. 电子与信息学报，2003，25(9)：1174-1179.

[2] 黄静霞，许慰玲，沈民奋. 基于独立分量分析的数字水印技术[J]. 计算机工程与科学，2004年，26(11)：42-46.

[3] 刘琚，张新刚，孙建德. 一种基于ICA的图像水印方法[J]. 电路与系统学报，2003，8(3)：55-59.

[4] NGUYEN TV, PATRA JC, CHAUDHARI NS. A novel digital image watermarking scheme using blind source separation[A]. International Conference on Image Processing(ICIP)[C]. 2004. 2649-2652.

[5] 刘琚，孙建德，张新刚. 基于ICA的数字水印的方法[J]. 电子学报，2004，32(4)：657-660.

[6] 王巍奇，付永生，李文明. 一种基于快速独立分量分析的图像水印算法[J]. 信号处理与模式识别，2005，(1)：10-12.

[7] 杨福生，洪波. 独立分量分析的原理与应用[M]. 北京：清华大学出版社，2006.101.

[8] 刘九芬，黄达人，王振武. 信息隐藏算法中的去噪[J]. 中山大学学报(自然科学版)，2002，41(5).