一种基于 ICA 的图像信息隐藏算法

赵 伟[1,2] 陈伟杰[1,2] 张晓玲[2]
(1 集美大学诚毅学院 厦门 361021;2 厦门大学通信工程系 厦门 361005)

摘 要: 独立分量分析(ICA)是一种基于高阶统计量的信号分析方法,它可以找到隐含在数据中的独立分量,已广泛应用于信号处理领域。信息隐藏是一种新兴的技术,其目的在于将秘密信息隐藏于另一非机密信息中。本文提出一种新的信息隐藏技术,即将 Arnold 置乱后的秘密图像嵌入到载体图像中,再利用 ICA 算法从中提取出秘密图像。仿真结果表明该算法有效可行。

关键词: 独立分量分析;信息隐藏;图像置乱;图像处理
中图分类号: TN911.73 文献标识码: A

Algorithm of information hiding based on ICA for image

Zhao Wei[1,2] Chen Weijie[1,2] Zhang Xiaoling[2]
(1 ChengYi College of Jimei University, Xiamen 361021;
2 Department of Communication Engineer, Xiamen University, Xiamen 361005)

Abstract: Independent Component Analysis (ICA) was widely used in signal processing, which is a signal analysis method based on signal's high order cumulants, it can find out the latent independent components in data. Information hiding technology is a new method in information processing; the hiding information is embed in public information. This paper introduces an algorithm based on ICA for information technology. This paper embeds the cryptogrammic hiding image in public image, then using ICA algorithm to abstract the hiding image. The results of emulation indicate this algorithm is available and feasible.

Keywords: independent component analysis; information hiding; image scrambling; image processing

0 引 言

随着计算机和网络技术的飞速发展,使多媒体信息交流达到了前所未有的深度和广度[1]。在开放的网络环境下,信息通信的安全问题引起了人们的极大关注,使得信息隐藏技术成为信息安全领域研究的热点。信息隐藏技术的意义在于将秘密信息隐藏于另一非机密信息中。它为在开放的网络环境下进行具有机密性质的数据通信、数字产品的版权认证和知识产权保护提供了可靠的信息安全保障。

独立分量分析(ICA)[2]是近年来迅速发展起来的基于统计独立思想从线性混合的观测信号中分离出独立信号源的一种技术,广泛应用于特征提取、盲源分离、语音处理、图像处理、生物医学及人脸识别[3-5]等许多领域。在图像处理方面其应用有:图像特征提取、图像去噪、人脸识别和检测、数字水印和遥感图像处理等,并且取得了令人满意的结果[6]。

1 独立分量分析

独立分量分析以非高斯源信号为研究对象,在对它们作统计独立假设条件下,将观测到的多路混合信号变换到相互独立的方向上,使经过变换所得到的各个分量之间不仅正交,而且相互独立。

ICA 的模型可描述为:假设 n 个相互独立的源信号 $s = [s_1, s_2, \cdots, s_n]^T$ 经过线性系统 A 混合在一起,得到 m 个观测信号 $x = [x_1, x_2, \cdots, x_m]^T$,源信号和观测信号之间满足如下关系式: $x = As$,其中 A 是一个 $m \times n$ 的矩阵。ICA 的目的是仅通过观测数据 x 估计出未知独立源 s 或估计出混合矩阵 A,即求解一个解混矩阵 w,使得 $y = wx = wAs = Gs = \hat{s}$ 的各分量尽可能相互独立,并把 y 作为源信号 s 的估计。

常用的 ICA 算法有:极大化非高斯性算法、非线性去相关算法、极大似然算法以及 FastICA 算法。目前,ICA 的主流算法是基于固定点的快速迭代算法(FastICA)[7]。

2　算法分析

本文提出一种基于 ICA 的数字图像信息隐藏算法：将载体图像分解成 4 个相关性很强的子图，再将置乱后的秘密图像嵌入到子图中，最后将子图按分解的逆过程还原成嵌有秘密信息的载体图像。嵌入算法和提取算法的具体流程如图 1、图 2 所示。

嵌入算法如下：

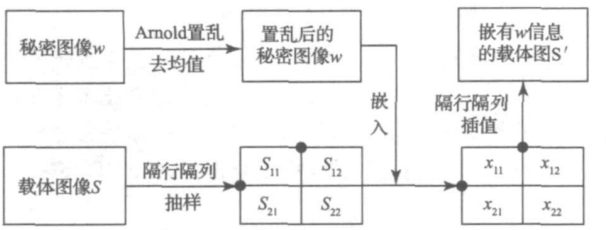

图 1　秘密图像嵌入算法

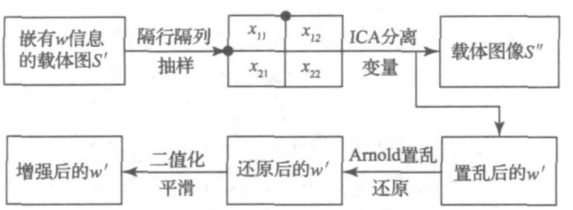

图 2　秘密图像提取算法

1) 对秘密图像 w 进行 Arnold 置乱[8]，并进行均值化处理；

2) 将载体图像 S 隔行隔列抽样成 4 个子图 S_{11}、S_{12}、S_{21}、S_{22}；

3) 将处理过的 w 分别嵌入到 4 个子图中，得到 4 个观测信号 x_{11}、x_{12}、x_{21}、x_{22}；

4) 将观测信号按隔行隔列顺序进行插值，得到嵌有 w 信息的载体图像 S'；

秘密图像提取算法：

1) 将 S' 按隔行隔列抽样得到四个观测信号；

2) 对观测信号利用 ICA 进行分离变量，得到载体图像 S'' 与置乱后的 $w'x;'$

3) 对 w′ 进行置乱还原；

4) 最后对 w′ 进行二值化和平滑滤波，得到增强后的秘密图像 w′。

2.1　秘密图像置乱

为了提高信息隐藏的隐蔽性，该算法将秘密图像进行置乱以达到加密的目的。图像置乱是将图像的位置进行变换使其转换成难以辩认的图像。目前使用较多的图像置乱变换方法有：Hilbert 曲线、空间填充曲线、幻方置乱变换、Arnold 变换等。本文采用具有周期性的 Arnold 变换对图像进行加密，并将其置换频率 f 作为密钥信息用于图像解密。所以即使嵌有秘密信息的图像遭到非法攻击者的拦截，也大大提高了其破解的难度。

为了让嵌入的秘密图像数据更像白噪声，本算法还将置乱后的图像去均值，即用置乱后的图像值减去秘密图像的平均值。

2.2　载体图像抽样及嵌入数据

通常的数字图像由于其领域间存在着很强的相关性，故可将载体图像 S 隔行和隔列抽样后的 4 个子图 S_{11}、S_{12}、S_{21}、S_{22} 近似看成同一幅图像，即：

$$S_{11} \approx S_{12} \approx S_{21} \approx S_{22} \tag{1}$$

将均值化处理后的 w 按式(2)分别嵌入到 4 个抽样子图中，得到观测信号 $X(x_{11}、x_{12}、x_{21}、x_{22})$。最后将观测信号分别按隔行隔列顺序进行插值成嵌有 w 信息的载体图像 S'。当嵌入的图像 w 强度较弱的情况下，图像具有较高的峰值信噪比，人眼主观上不易察觉其变化，因此在开放的网络里不易引起不法拦截者的注意，使得秘密图像得到安全的传输。

$$\begin{cases} x_{11} = S_{11} + a_1 \times w \\ x_{12} = S_{12} + a_2 \times w \\ x_{21} = S_{21} + a_3 \times w \\ x_{22} = S_{22} + a_4 \times w \end{cases} \tag{2}$$

式中：a_1、a_2、a_3、a_4 分别为嵌入的强度。

2.3　提取秘密图像

由于 S_{11}、S_{12}、S_{21}、S_{22} 具有较强的相关性，如式(1)，所以可以把观测信号 X 近似为独立变量 S 和 w 的线性混合，进而可以采用 ICA 算法从观测信号中分离出 w。

秘密信息的提取算法是嵌入算法的逆过程。首先将图像 S' 进行隔行和隔列抽样观测信号 X；接着利用 FastICA 算法从观测信号中分离出载体图像 S'' 和置乱后的秘密图像 w'；最后利用置乱频率 f 还原出秘密图像。但是由于式(1)的近似性，使得还原出的 w' 具有较强的噪声。为了提高 w' 可读性，本算法先计算 w' 的平均值 t，再按式(3)进行二值化处理。为进一步抑制噪声，还对其进行平滑滤波。

$$\begin{cases} w'(i,j) = 1 & w'(i,j) \leqslant t \\ w'(i,j) = 0 & w'(i,j) > t \end{cases} \tag{3}$$

式中：t 为 w' 的平均值。

3　算法仿真与分析

本文以 256 × 256 大小的 Lena 图像为载体 S，将作者个人信息制成的二值图像作为秘密图像 w，在 Matlab 下进行仿真实验。

图 3 为 Lena 载体图像及其隔行和隔列抽样所得的 4 个子图 S_{11}、S_{12}、S_{21}、S_{22}，将子图转化成一维矢量后，计算各子图间的归一化相关系数，如表 1 所示。由表 1 可知各子图间具有很强的相关性，因此式(1)的近似假设是成立的。

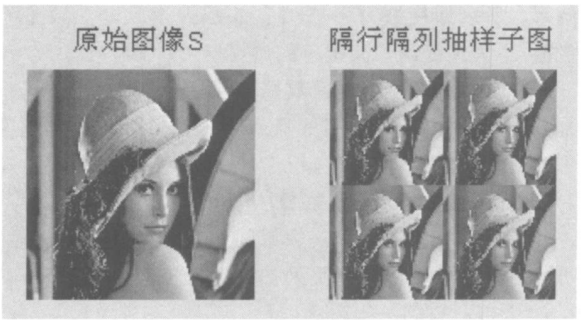

图 3　载体及其抽样图像

表 **1**　子图的归一化相关系数

	S_{11}	S_{12}	S_{21}	S_{22}
S_{11}	1.0000	0.9270	0.9625	0.9060
S_{12}	0.9270	1.0000	0.9276	0.9616
S_{21}	0.9625	0.9276	1.0000	0.9265
S_{22}	0.9060	0.9616	0.9265	1.0000

原始的秘密图像 w、置乱均值化后的 w 以及嵌有 w 信息的 Lena 图像, 如图 4 所示。嵌入的强度选取 $a_1 = a_4 = 0.017$, $a_2 = a_3 = -0.017$ 时, Lena 图 S 与 S' 的峰值信噪比(PSNR)值为 42.1209, 人眼不易察觉 S' 中含有异常信息。

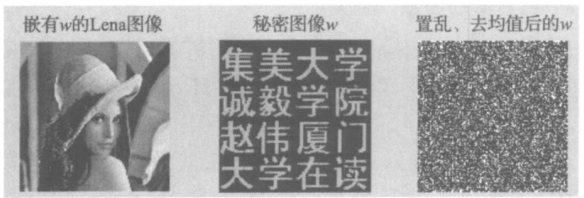

图 4　含秘密信息的图像

利用提取算法从 S' 中提取的秘密图像 w'、二值化处理后的 w' 以及平滑处理后的 w', 如图 5 所示。原始的秘密图像 w 与增强处理后图像 w' 的归一化相关系数为 0.7482。从图 5 可以准确无误的识别出作者的个人信息。

图 5　提取的秘密图像

提高 w 的嵌入强度, 可以明显地增强提取出的 w' 的可读性, 但却降低的载体的峰值信噪比。当 $a_1 = a_4 = 0.025$, $a_2 = a_3 = -0.025$ 时, S 与 S' 的峰值信噪比为 38.7711, 提取的 w 的相关性为 0.7922, 效果如图 6 所示。

图 6　提高嵌入强度的 w 提取图像

4　结　　论

在开放的网络中, 秘密信息的安全传输是个很重要的问题。本文提出的基于 ICA 的图像信息隐藏技术为此提供了一个性能良好的简易可行的解决方案, 即使载体图像遭到非法攻击者的拦截, 其秘密信息也很难被破译出来。

参 考 文 献

[1] 路亚峰, 张贤, 赵玉奎, 等. 数字水印技术研究[J]. 电子测量技术, 2009, 32(8): 95-99.

[2] COMON P. Independent component analysis-a new concept [J]. Signal Processing, 1994, 36: 287-314.

[3] 杨科化, 柳重堪. 基于独立分量分析的数字水印攻击[J]. 仪器仪表学报, 2004, 25(4): 547-548.

[4] 游荣义, 陈忠. 基于小波变换的盲信号分离的神经网络方法[J]. 仪器仪表学报, 2005, 26(4), 415-418.

[5] 黄璞, 陈才扣. 基于二维图像矩阵的 ICA 人脸识别[J]. 计算机工程与设计, 2009, 30(24): 5686-5688.

[6] 郭武, 张鹏, 王润生. 独立分量分析在图像处理中的应用现状[J]. 计算机工程与应用, 2008, 44 (23): 172-176.

[7] HYVARINEN A, KARHUNEN J, OJAE. Independent Component Analysis [M]. JohnWiley& Sons. Inc, 2001.

[8] 李志伟, 陈燕梅, 张胜元. 基于 SNR 的数字图像置乱程度评价方法[J]. 厦门大学学报, 2006, 45(7), 484-487.

作 者 简 介

赵伟, 男, 助理实验师, 厦门大学在读研究生, 主要研究方向为信号处理、嵌入式系统开发与应用等。

E-mail: zhaowei701@163.com