# 基于盲源分离的多幅顺序图像加密方法

党　杰　　林秋华　　殷福亮
(大连理工大学子与信息工程学院　大连　116023)

**摘　要**：根据许多加密方法利用数学难题保障其安全性的思想，盲源分离欠定难题可用于高度安全的多幅图像加密。然而，由于盲源分离存在顺序和幅度模糊性，通过盲源分离得到的解密图像可能发生顺序变化和像素值反转。这在加密多幅顺序图像时可能导致解密错误。针对这一问题，该文利用数字水印技术，加密前在每幅明文图像中嵌入与其对应的顺序信息；解密后，通过在各解密图像中检测该顺序信息而消除其顺序和幅度的模糊性。计算机仿真结果表明，该方法在恢复解密图像顺序的同时也能检测其是否反转，从而有效地解决了多幅顺序图像的盲源分离加密问题。

**关键词**：图像加密；数字水印；盲源分离；模糊性；顺序信息
**中图分类号**：TP391　　**文献标识码**：A　　**文章编号**：1009-5896(2007)06-1471-05

# Encryption of Multiple Sequential Images Using Blind Source Separation

Dang Jie　　Lin Qiu-hua　　Yin Fu-liang
(*School of Electronic and Information Engineering*, *Dalian University of Technology*, *Dalian* 116023, *China*)

**Abstract**: Since the security of many cryptosystems relies on the apparent intractability of the computational problems, the underdetermined problem of Blind Source Separation (BSS) is used to encrypt multiple images with high security. However, due to the BSS ambiguity, the order of BSS decrypted images may different from that of the original images and the value of pixel in some decrypted images may be reversed, which can result in decryption errors when encrypting multiple sequential images. To solve this problem, digital watermarking technique is utilized to embed some order information into each original image before encryption. After decryption, these order information is extracted from the decrypted images and then used to eliminate the decryption errors. Computer simulation results show that the proposed method not only can recover the original order of the decrypted images, but also can detect if the decrypted images are reversed.

**Key words**: Image encryption; Digital watermarking; Blind source separation; Ambiguity; Order information

## 1　引言

盲源分离(Blind Source Separation, BSS)是最近十几年来信号处理方面的热门研究领域。它可以不用任何先验知识，仅仅利用源信号相互独立的假设，就能从一组可观测的源信号的混合信号中恢复出各源信号。这种解决问题的独特方式使它在通信信号处理、生物医学信号处理、图像处理等许多领域有着广泛而重要的应用[1–3]。

在盲源分离各种应用中，为保证源信号的可分离性，通常要求混合信号个数多于源信号个数。这是因为当混合信号个数少于源信号个数时，盲源分离通常不可能完全分开所有的源信号[4]，这就是求解极为困难的盲源分离欠定难题(underdetermined BSS problem)。然而，在密码学上，许多加密方法正是利用了数学难题来保障其安全性。根据这一设计思想，文献[5]利用盲源分离欠定难题提出了一种新的多幅图像加密方法。该方法的中心思想是，在加密过程中通过应用密钥图像设置盲源分离欠定难题，在解密时再利用密钥图像解决这一难题。由于密钥图像与明文图像大小相等数目相同，根据 Shannon 关于密码学的理论，该加密方法已具备无条件安全的必要条件[6]。若密钥图像随机性好，该方法具有极高的安全性。

然而，由于盲源分离输出信号存在顺序和幅度模糊性，通过盲分离得到的解密图像的顺序与加密前相比可能发生变化，有些图像的像素值还可能反转。因此，要想得到正确的解密图像，必须在文献[5]中原有方法基础上增加一定的加密预处理和解密后处理。为此，本文利用数字水印技术，加密前在明文图像中嵌入顺序信息，并通过在解密图像中检测该顺序信息来恢复出加密前的多幅顺序图像。计算机仿真实验结果验证了本文方法的有效性。

## 2　基于盲源分离的多幅图像加密方法

多幅图像的盲源分离加密方法的原理框图如图 1 所

2005-10-26 收到，2006-04-20 改回
国家自然科学基金(60402013；60372082)资助课题

示[5]。其中 $s_1(t),\cdots,s_P(t)$ , $t=1,\cdots,T$, 表示 $P$ 幅被同时加密的明文图像的一维数据， $T$ 为数据长度(对应各图像的大小)。$s_{n1}(t),\cdots,s_{nP}(t)$ 是 $P$ 幅相互统计独立的密钥图像的一维数据，由均匀分布的随机数组成。这些随机数则由随机数发生器生成，并由密钥种子 $I_0$ 初始化。 $x_1(t),\cdots,x_P(t)$ 是 $P$ 幅用于传输的加密图像的一维数据，$\hat{s}_1(t),\cdots,\hat{s}_P(t)$ 表示 $P$ 幅盲源分离解密图像的一维数据。

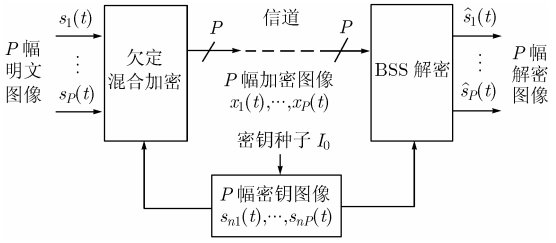


图 1 盲源分离图像加密方法原理框图

### 2.1 欠定混合加密

首先构造一个 $P\times 2P$ 欠定混合加密阵[5]：

$$\boldsymbol{A}_e=[\boldsymbol{B}\quad \beta\boldsymbol{B}] \tag{1}$$

其中 $\boldsymbol{B}$ 是一个 $P\times P$ 满秩方阵，由$(-1,1)$间均匀分布的随机数生成。$\beta$ 为一个标量值。为保障明文图像被密钥图像以高能量所覆盖，取 $\beta\geq 10$ 。然后，将 $P$ 幅明文图像 $s_1(t),\cdots,s_P(t)$ 和 $P$ 幅密钥图像 $s_{n1}(t),\cdots,s_{nP}(t)$ 在欠定混合加密阵 $\boldsymbol{A}_e$ 作用下进行混合，得到 $P$ 幅加密图像 $x_1(t),\cdots,x_P(t)$ ：

$$\boldsymbol{x}_P(t)=\boldsymbol{A}_e\ \boldsymbol{s}_{2P}(t) \tag{2}$$

其中 $\boldsymbol{x}_P(t)=[x_1(t),\cdots,x_P(t)]^{\mathrm{T}}$ ， $\boldsymbol{s}_{2P}(t)=[s_1(t),\cdots,s_P(t),s_{n1}(t),\cdots,s_{nP}(t)]^{\mathrm{T}}$ 。显然，对于没有 $P$ 幅密钥图像的非法用户而言，该加密过程设置了盲源分离欠定难题：$2P$ 个源信号，$P$ 个混合信号。

Cao 和 Liu 在文献[4]中指出，仅当可观测的混合信号满足一定条件时，盲源分离算法才能够分离源信号，这叫做源信号的可分离性(separability)。而且，他们提出并证明了源可分离性与混合矩阵结构有关的 $L$ 行可分解($L$-row decomposable)定理。基于该定理，文献[7]证明了式(1)中的欠定混合加密阵 $\boldsymbol{A}_e$ 具有源不可分离性。也就是说，如果没有 $P$ 幅密钥图像，非法用户将无法通过盲源分离从 $P$ 幅加密图像中恢复 $P$ 幅明文图像。

### 2.2 BSS 解密

在接收端，将 $P$ 幅加密图像 $x_1(t),\cdots,x_P(t)$ 和 $P$ 幅再生密钥图像 $s_{n1}(t),\cdots,s_{nP}(t)$ 组合成 $2P$ 幅混合图像 $\boldsymbol{x}_{2P}(t)$ 进行盲源分离，即 $\boldsymbol{x}_{2P}(t)=[x_1(t),\cdots,x_P(t),s_{n1}(t),\cdots,s_{nP}(t)]^{\mathrm{T}}$ 。根据式(2)有

$$\boldsymbol{x}_{2P}(t)=\boldsymbol{A}_d\ \boldsymbol{s}_{2P}(t) \tag{3}$$

式中 $\boldsymbol{A}_d$ 为等效的解密混合矩阵：

$$\boldsymbol{A}_d=\begin{bmatrix}\boldsymbol{B} & \beta\boldsymbol{B}\\ \boldsymbol{0} & \boldsymbol{I}\end{bmatrix} \tag{4}$$

其中 $\boldsymbol{0}$ 和 $\boldsymbol{I}$ 分别为 $P\times P$ 维零阵和单位阵。显然， $\boldsymbol{A}_d$ 为 $2P\times 2P$ 维方阵。这就是说，加密时的盲源分离欠定难题已在解密过程中转化为最简单的盲源分离情况：$2P$ 个源信号，$2P$ 个混合信号。因此，包括 $P$ 幅明文图像和 $P$ 幅密钥图像在内的所有 $2P$ 个源信号都能得以完全分离，从而给出 $P$ 幅解密图像 $\hat{s}_1(t),\cdots,\hat{s}_P(t)$ 。

### 2.3 顺序和幅度模糊性在解密图像中的表现

由于盲源分离没有利用任何先验知识，致使盲源分离输出信号与源信号相比具有顺序和幅度模糊性[8, 9]。对于基于盲源分离的图像加密而言，两种模糊性表现在：(1)与 $P$ 幅明文图像 $s_1(t),\cdots,s_P(t)$ 相比， $P$ 幅盲源分离解密图像 $\hat{s}_1(t),\cdots,\hat{s}_P(t)$ 的顺序发生变化；(2)其中某些图像的像素值反转。

当加密多幅顺序图像时，上述两种模糊性可能导致解密错误。为此，必须在多幅明文图像中引入顺序的先验知识(即嵌入顺序信息)，并通过解密后提取、检测该顺序信息，有效解决解密图像的顺序变化和像素值反转问题。

## 3 利用数字水印技术消除解密模糊性

数字水印具有视觉不可见性、鲁棒性和易提取性等 3 种性能[10]。这使得数字水印技术非常适于在多幅顺序明文图像中嵌入顺序信息，进而解决多幅顺序图像的加密问题。首先，视觉不可见性使明文图像在加入顺序信息后不发生任何视觉上的改变；其次，鲁棒性使顺序信息在盲源分离解密处理后不被破坏；最后，易提取性又使顺序信息很方便地从解密图像中检测出来，从而快速确定解密图像的顺序和像素值反转问题。

本文采用了基于 DCT 域的扩展谱水印技术[11]，在图像子块(8×8)的直流(DC)系数上嵌入顺序信息。文献[12]阐明了 DC 系数上嵌入信息的有效性。考虑到在图像加密应用背景下，顺序信息嵌入应本着在确保恢复的条件下嵌入数据量较小的原则，本文仅选择了 DC 系数最大的一部分图像子块进行顺序信息嵌入。这是因为在视觉不可见的前提下，大的 DC 系数具有较大的可改变范围，或者说有较大的信息嵌入强度，这能使检测错误率进一步下降。与此嵌入方案相对应，本文给出了与文献[12]不同的顺序信息检测器。

下面将详细介绍每幅明文图像(简称 $s$)的顺序信息嵌入、顺序信息提取、顺序恢复和反转图像检测等 3 个过程。

### 3.1 顺序信息嵌入

顺序信息嵌入过程主要包括明文图像分块、顺序信息嵌入和 DCT 反变换等 3 个步骤。

(1) 明文图像分块：将明文图像 $s$ 首先分割成互不覆盖的 8×8 图像子块，记为 $M_j$ ，其中 $j=1,\cdots,K$ ，它表示各子块在图像中的位置， $K$ 表示图像子块总数。

(2) 顺序信息嵌入：首先，对每一图像子块 $M_j$ 进行 DCT 变换：

$$D_j(u,v)=\mathrm{DCT}(M_j),\quad 1\leq u,v\leq 8 \tag{5}$$

则各块的 DC 系数 $D_j(1,1)$ 组成向量 $\boldsymbol{D}=[D_1(1,1),D_2(1,1),\cdots,$

$D_K(1,1)]$。然后，从 $\boldsymbol{D}$ 中找出 $L$ ( $L<K$ )个较大的 DC 系数 $\boldsymbol{D}^*=[D_1^*(1,1), D_2^*(1,1), \cdots, D_L^*(1,1)]$，且 $D_1^*(1,1)\ge D_2^*(1,1)\ge \cdots \ge D_L^*(1,1)$。因为 $D_i^*(1,1)\in \boldsymbol{D}$，$i=1,\cdots,L$，所以 $D_i^*(1,1)$ 仍可记录其对应的块，即 $j$ 的值。

本文嵌入的顺序信息 $\boldsymbol{\omega}$ 由均值为 0、方差为 1 的高斯分布随机序列构成，长度也为 $L$，即 $\boldsymbol{\omega}=[\omega_1,\omega_2,\cdots,\omega_L]$。通过改变 $D_i^*(1,1)$，得到嵌入了顺序信息的 DC 系数 $D_i'(1,1)$ 如下：

$$D_i'(1,1)=D_i^*(1,1)(1+\alpha\omega_i),\quad i=1,\cdots,L \tag{6}$$

其中 $\alpha$ 为嵌入比例因子。由于较大的 DC 系数在图像中代表亮度大、表面平坦的区域，故 $\alpha$ 的选择较其他水印嵌入方法应小一些，例如 $\alpha\le 0.015$ [12]。

(3) DCT 反变换：除了 $D_i'(1,1)$ 嵌入了顺序信息外，与 $D_i'(1,1)$ 是同一块的 AC 系数以及没有被选到块的 DCT 系数均保持不变。若记此时全部子块的 DCT 系数为 $D_j'(u,v)$，对其进行 DCT 反变换：

$$G_j=\mathrm{IDCT}(D_j'(u,v)) \tag{7}$$

由 $G_j$ 可构成嵌入了顺序信息的明文图像 $s^*$。

至此，DC 系数 $\boldsymbol{D}^*$，位置信息 $j$，嵌入的顺序信息 $\boldsymbol{\omega}$ 和嵌入比例因子 $\alpha$ 共同组成了明文图像 $s$ 的顺序检测信息 $\boldsymbol{\eta}$。若有 $P$ 幅顺序明文图像，则它们的顺序检测信息对应为 $\boldsymbol{\eta}_k$，$k=1,\cdots,P$。与 $P$ 幅明文图像相比，$\boldsymbol{\eta}_k$ 的数据量很小，可与加密数据一起发送到接收端，用于在解密图像中提取、检测顺序信息，进而恢复其原始顺序并判断其反转情况。

### 3.2 顺序信息提取

顺序信息提取过程包括解密图像分块和顺序信息提取两个步骤。

(1) 解密图像分块：对盲源分离解密图像 $\hat{s}$ 及其反转图像 $\hat{s}'$ 进行和明文图像一样的分块操作，得到图像子块 $\tilde{G}_j$ 和 $\tilde{G}_j'$。利用顺序检测信息 $\boldsymbol{\eta}_k$ 中的位置信息容易从 $\tilde{G}_j$ 和 $\tilde{G}_j'$ 中定位可能嵌有 $\boldsymbol{\eta}_k$ 中顺序信息 $\boldsymbol{\omega}_k$ 的图像子块 $\tilde{G}_i$ 和 $\tilde{G}_i'$，$i=1,\cdots,L$。

(2) 顺序信息提取：对 $\tilde{G}_i$ 和 $\tilde{G}_i'$ 分别进行 DCT 变换，

$$\tilde{F}_i(u,v)=\mathrm{DCT}(\tilde{G}_i),\ \tilde{F}_i'(u,v)=\mathrm{DCT}(\tilde{G}_i') \tag{8}$$

由于 $\boldsymbol{\eta}_k$ 记录了对应 $\tilde{G}_i$ 和 $\tilde{G}_i'$ 的原始 DC 系数 $D_i^*(1,1)$ 和嵌入比例因子 $\alpha$，根据式(6)，$\hat{s}$ 和 $\hat{s}'$ 嵌入的顺序信息可由下式提取：

$$\tilde{\omega}_i=\frac{\tilde{F}_i(1,1)\big/D_i^*(1,1)-1}{\alpha},\quad \tilde{\omega}_i'=\frac{\tilde{F}_i'(1,1)\big/D_i^*(1,1)-1}{\alpha} \tag{9}$$

### 3.3 顺序恢复和反转图像检测

设从 $\hat{s}$ 和 $\hat{s}'$ 提取的顺序信息分别为 $\tilde{\boldsymbol{\omega}}=[\tilde{\omega}_1,\tilde{\omega}_2,\cdots,\tilde{\omega}_L]$ 和 $\tilde{\boldsymbol{\omega}}'=[\tilde{\omega}_1',\tilde{\omega}_2',\cdots,\tilde{\omega}_L']$，并记 $\tilde{\boldsymbol{\omega}}$，$\tilde{\boldsymbol{\omega}}'$ 和 $\boldsymbol{\eta}_k$ 记录的顺序信息 $\boldsymbol{\omega}_k$ 去均值后的对应变量为 $\tilde{\boldsymbol{\nu}}$，$\tilde{\boldsymbol{\nu}}'$ 和 $\boldsymbol{\nu}_k$，则 $\tilde{\boldsymbol{\omega}}$ 与 $\boldsymbol{\omega}_k$ 以及 $\tilde{\boldsymbol{\omega}}'$ 与 $\boldsymbol{\omega}_k$ 的归一化相关系数如下：

$$\rho(\tilde{\boldsymbol{\omega}},\boldsymbol{\omega}_k)=\frac{\tilde{\boldsymbol{\nu}}\boldsymbol{\nu}_k^{\mathrm{T}}}{\sqrt{\tilde{\boldsymbol{\nu}}\tilde{\boldsymbol{\nu}}^{\mathrm{T}}}\sqrt{\boldsymbol{\nu}_k\boldsymbol{\nu}_k^{\mathrm{T}}}},\quad \rho(\tilde{\boldsymbol{\omega}}',\boldsymbol{\omega}_k)=\frac{\tilde{\boldsymbol{\nu}}'\boldsymbol{\nu}_k^{\mathrm{T}}}{\sqrt{\tilde{\boldsymbol{\nu}}'\tilde{\boldsymbol{\nu}}'^{\mathrm{T}}}\sqrt{\boldsymbol{\nu}_k\boldsymbol{\nu}_k^{\mathrm{T}}}} \tag{10}$$

其中 $0\le\left|\rho(\tilde{\boldsymbol{\omega}},\boldsymbol{\omega}_k)\right|\le 1$，$0\le\left|\rho(\tilde{\boldsymbol{\omega}}',\boldsymbol{\omega}_k)\right|\le 1$。显然，如果该解密图像中嵌有顺序信息 $\boldsymbol{\omega}_k$ 时，$\rho(\tilde{\boldsymbol{\omega}},\boldsymbol{\omega}_k)$ 和 $\rho(\tilde{\boldsymbol{\omega}}',\boldsymbol{\omega}_k)$ 中有且只有一个接近于 1 的正值，否则，两者的绝对值都远小于 1。

检测解密图像顺序和反转的具体方法如下：设定阈值 $\xi$，将 $\rho(\tilde{\boldsymbol{\omega}},\boldsymbol{\omega}_k)$ 和 $\rho(\tilde{\boldsymbol{\omega}}',\boldsymbol{\omega}_k)$ 与 $\xi$ 进行比较：若 $\rho(\tilde{\boldsymbol{\omega}},\boldsymbol{\omega}_k)\ge\xi$，则解密图像 $\hat{s}$ 是第 $k$ 幅明文图像，或若 $\rho(\tilde{\boldsymbol{\omega}}',\boldsymbol{\omega}_k)\ge\xi$，则解密图像的反转图像 $\hat{s}'$ 是第 $k$ 幅明文图像，即解密图像 $\hat{s}$ 是反转图像；否则，若 $\left|\rho(\tilde{\boldsymbol{\omega}},\boldsymbol{\omega}_k)\right|<\xi$ 且 $\left|\rho(\tilde{\boldsymbol{\omega}}',\boldsymbol{\omega}_k)\right|<\xi$，则解密图像 $\hat{s}$ 不是第 $k$ 幅明文图像。

## 4 仿真结果

为表明本文方法的有效性，我们进行了大量的计算机仿真实验。其中的一个实验是，对图 2(a)所示 3 幅有顺序头像 $s_1$，$s_2$ 和 $s_3$ 进行盲源分离加密。

首先，按照本文第 3 节介绍的方法，在 3 幅顺序明文图像 $s_1$，$s_2$ 和 $s_3$ 中嵌入顺序信息。如上所述，在顺序图像加密应用中，要求在明文图像中嵌入的顺序信息量应较小，而且要求在解密图像中能有效检测该信息。综合考虑这两方面的

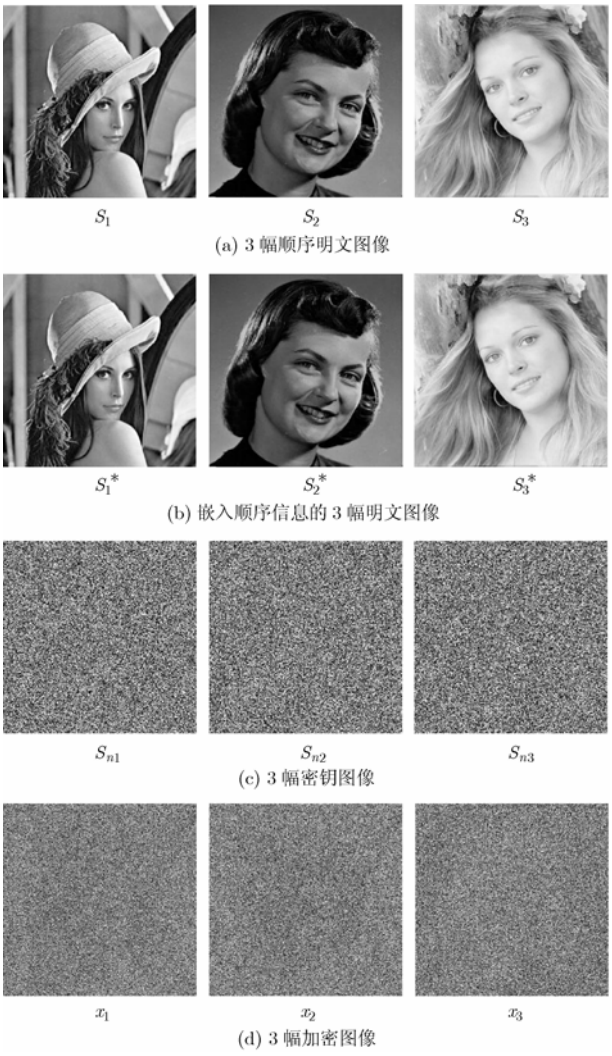


图 2　3 幅顺序明文图像的加密实验

要求，较大 DC 系数的个数 $L$ 选在 10～20 之间为好。为了进一步减少检测错误率，本文对 3 幅明文图像嵌入了不同长度的顺序信息 $\boldsymbol{\omega}_i(i=1,2,3)$，其长度分别为 $L_1=10$，$L_2$=12，$L_3=14$。同时取 $\alpha=0.01$。嵌入了顺序信息的 3 幅明文图像 $s_1^*$，$s_2^*$ 和 $s_3^*$ 如图2(b)所示。与原始图像 $s_1$，$s_2$ 和 $s_3$ 相比，$s_1^*$，$s_2^*$ 和 $s_3^*$ 并未发生任何可见的改变。至此，容易得到 3 幅明文图像的顺序信息 $\boldsymbol{\eta}_i$，$i=1,2,3$，它们代表了明文图像的原始顺序。

将 $s_1^*$，$s_2^*$ 和 $s_3^*$ 在欠定混合加密阵 $\boldsymbol{A}_e$ 作用下与图 2(c) 中的 3 幅密钥图像 $s_{n1}$，$s_{n2}$ 和 $s_{n3}$ 进行混合加密，得到 3 幅加密图像 $x_1$，$x_2$ 和 $x_3$，如图 2(d)所示。经过通信传输后，在接收端通过重构密钥图像 $s_{n1}$，$s_{n2}$ 和 $s_{n3}$，便可应用盲源分离算法对加密图像 $x_1$，$x_2$ 和 $x_3$ 进行解密。为了更好地验证本文方法的有效性，这里运用了 3 种不同的盲源分离算法进行解密。它们分别是 ComonICA[8]，FastICA[1]和 SANG[2]算法。3 种算法得到的解密图像分别如图 3(a)，图 3(b)和图 3(c)所示。可见，用 3 种盲源分离算法得到的 3 组解密图像的顺序各不相同，而且某些图像的像素值反转了。

为了正确有效地恢复出加密前的多幅顺序图像，本文基于第 3 节提出的方法，应用顺序检测信息 $\boldsymbol{\eta}_i(i=1,2,3)$，分别对 3 种盲源分离算法的解密图像及其反转图像进行了顺序信息检测，得到了表 1 所示的检测结果。设定阈值 $\xi$=0.7，从表 1 中容易看出 3 幅解密图像 $\hat{s}_1,\hat{s}_2,\hat{s}_3$ 与 3 幅明文图像的顺序对应关系。以 ComonICA 算法得到的 3 幅解密图像为例，用 $\boldsymbol{\eta}_1$ 在解密图像 $\hat{s}_2$ 中检测到了顺序信息 $\boldsymbol{\omega}_1$，检测值是 0.96，而在 $\hat{s}_1$ 和 $\hat{s}_3$ 中的检测值都很小。这说明解密图像 $\hat{s}_2$ 就是顺序明文图像的第 1 幅图像。同理可得解密图像 $\hat{s}_3$ 是第 2 幅明文图像。对于解密图像 $\hat{s}_1$，在其中检测到了负的相关系数峰值，而在其反转图像中检测到了正的相关系数峰值。这说明 $\hat{s}_1$ 已反转，即其反转图像是明文顺序图像的第 3 幅。上


图 3 3 种盲源分离算法得到的 3 组解密图像( $\hat{s}_1$，$\hat{s}_2$ 和 $\hat{s}_3$ )

述检测结果的正确性容易通过比较图 3(a)和图 2(a)得到验证。

对 FastICA 和 SANG 算法对应的解密图像做同样的分析，可以得到同样正确的恢复结果，即 FastICA 算法已经给出了正确的解密图像顺序，而且没有图像发生像素值反转；而 SANG 算法得到的解密图像顺序是 1，3，2，且第 1 幅解密图像 $\hat{s}_1$ 的像素值发生了反转，具体如表 1 所示。总之，上述仿真结果表明，对于不同盲源分离算法得到的解密图像，本文方法都能够通过顺序信息提取和检测，完全消除解密图像的顺序和幅度模糊性，从而正确地恢复出加密前的多幅顺序图像。

**表 1 ComonICA，FastICA 和 SANG 等 3 种 BSS 算法解密图像的顺序和反转情况检测结果**

| | | $\hat{s}_1$ | | $\hat{s}_2$ | | $\hat{s}_3$ | |
|---|---|---|---|---|---|---|---|
| | | 解密图像 | 反转图像 | 解密图像 | 反转图像 | 解密图像 | 反转图像 |
| ComonICA | $\boldsymbol{\eta}_1$ | 0.28 | −0.26 | **0.96** | −0.65 | 0.09 | −0.08 |
| | $\boldsymbol{\eta}_2$ | −0.29 | 0.19 | 0.26 | −0.31 | **0.96** | −0.44 |
| | $\boldsymbol{\eta}_3$ | **−0.93** | **0.99** | 0.17 | −0.17 | −0.47 | 0.47 |
| FastICA | $\boldsymbol{\eta}_1$ | **0.96** | −0.64 | 0.09 | −0.08 | −0.26 | 0.28 |
| | $\boldsymbol{\eta}_2$ | 0.26 | −0.31 | **0.95** | −0.45 | 0.19 | −0.29 |
| | $\boldsymbol{\eta}_3$ | 0.17 | −0.17 | −0.47 | 0.47 | **0.99** | **−0.93** |
| SANG | $\boldsymbol{\eta}_1$ | −0.67 | **0.93** | −0.25 | 0.28 | 0.10 | −0.09 |
| | $\boldsymbol{\eta}_2$ | −0.31 | 0.27 | 0.20 | −0.30 | **0.73** | −0.40 |
| | $\boldsymbol{\eta}_3$ | −0.16 | 0.16 | **0.86** | **−0.82** | −0.45 | 0.46 |

## 5　结束语

本文利用数字水印技术，通过加密前对明文顺序图像进行顺序信息嵌入预处理，以及在解密后的顺序信息提取和检测后处理，有效地解决了盲源分离加密方法中解密图像的顺序模糊性和像素值反转问题。此外，顺序信息的嵌入位置和长度可以根据具体情况进行具体选择，从而能进一步降低误检率。计算机仿真结果表明了本文方法的有效性。

## 参 考 文 献


[1] Hyvärinen A, Karhunen J, and Oja E. Independent Component Analysis. New York: John Wiley, 2001, chapter1, chapter8.

[2] Cichocki A and Amari S. Adaptive Blind Signal and Image Processing: Learning Algorithms and Applications. Chichester: John Wiley, 2003, chapter1, chapter6.

[3] Cardoso J F. Blind signal separation: statistical principles. *Proc. IEEE*, 1998, 86(10): 2009–2025.

[4] Cao X R and Liu R W. General approach to blind source separation. *IEEE Trans. on Signal Processing*, 1996, 44(3): 562–571.

[5] Lin Q H, Yin F L, and Liang H L. Blind source separation-based encryption of images and speeches. Lecture Notes in Computer Science, Berlin: Springer, 2005, 3497: 544–549.

[6] 杨波. 现代密码学. 北京: 清华大学出版社, 2003: 8–9.

[7] Lin Q H, Yin F L, Mei T M, and Liang H L. A blind source separation based method for speech encryption. *IEEE Trans. on Circuits and Systems* I, 2006 (in press).

[8] Comon P. Independent component analysis, a new concept? *Signal Processing*, 1994, 36(3): 287–314.

[9] Tong L, Liu R W, Soon V C, and Huang Y F. Indeterminacy and identifiability of blind identification. *IEEE Trans. on Circuits and Systems*, 1991, 38(5): 499–509.

[10] Barni M. What is the future for watermarking? *IEEE Signal Processing Magazine,* 2003, 20(5): 55–60.

[11] Cox I J, Kilian J, Leighton T, and Shamoon T. Secure spread spectrum watermarking for images, audio and video. Proc. of IEEE Int. Conf. on Image Processing, Lausanne, Switzerland, 1996: 243–246.

[12] 黄继武, Shi Y Q, 程卫东. DCT 域图像水印: 嵌入对策和算法. 电子学报，2000, 28(4): 57–60.
Huang Ji-wu, Yun Q.Shi, and Cheng Wei-dong. Image watermarking in DCT: An embedding strategy and algorithm. *Acta Electronica Sinica*, 2000, 28(4): 57–60.



党　杰：　男，1982年生，硕士生，研究方向为数字图像处理.

林秋华：　女，1969年生，博士，副教授，主要从事盲信号处理和信息安全等领域的研究.

殷福亮：　男，1962年生，教授，博士生导师，主要从事通信信号处理和阵列信号处理等领域的研究.