

基于迭代混合的数字图像隐藏技术

张贵仓¹⁾ 王让定²⁾ 章毓晋³⁾

¹⁾西北师范大学信息与计算科学系 兰州 730070)

²⁾宁波大学信息学院 宁波 315211)

³⁾清华大学电子工程系 北京 100084)

摘 要 提出了数字图像的单幅迭代混合和多幅迭代混合思想.利用图像的迭代混合可以将一幅图像隐藏于另一幅图像之中,多幅迭代混合可将一幅图像通过一组图像隐藏起来,迭代混合参数还可以作为隐藏图像的密钥,极大地提高了系统的安全性和隐藏图像的健壮性,图像迭代混合思想还可以应用到数字水印的研究与应用中.实验分析显示,该方法简单易行,并且算法具有一定程度的鲁棒性.

关键词 数字图像;信息隐藏;混合;迭代;数字水印

中图法分类号 TP391

Digital Image Information Hiding Technology Based on Iterative Blending

ZHANG Gui-Cang¹⁾ WANG Rang-Ding²⁾ ZHANG Yu-Jin³⁾

¹⁾Department of Information and Computing Science, Northwest Normal University, Lanzhou 730070)

²⁾College of Information, Ningbo University, Ningbo 315211)

³⁾Department of Electronic Engineering, Tsinghua University, Beijing 100084)

Abstract The digital image blending is introduced, and the single iterative digital image blending and multiple iterative digital image blending are firstly proposed. With the digital image iterative blending, new kinds of digital image information hiding schemes are presented. Firstly, with the single iterative image blending, a secret image can be hidden in one carrier image, a self-adaptive image hiding algorithm is obtained. The carrier image and the blending parameter can act as the private keys. But, if a malicious attacker get the carrier image and the blending image, it is totally possible for him to recover the secret image. So authors developed the multiple iterative image blending, with which a secret image can be hidden in one carrier image through many images. An image hiding algorithm is obtained. The blending images and the blending parameters and the sequences of the images blended can act as the private keys. It is impossible for an attacker to get all the blending images and the blending parameters, even if the attacker get all the blending images and parameters, he still can not recover the secret image due to the lack of the processes of the blending. Furthermore, the single iterative image blending scheme and the multiple iterative image blending scheme can be used together, which could much more enhance the security and robustness of the hidden image. In order to even more enhance the security and robustness of the hidden image, the scrambling technology can be used as pre-process and post-process of digital image information hiding. The examples show that the schemes can be expediently realized and they are robust in some extent. The techniques also can be used in digital water-

收稿日期:2002-01-15;修改稿收到日期:2003-01-23.本课题得到西北师范大学“知识与科技创新工程”项目(NWNU-KJ CXGC-02-13)及浙江省创新项目(ZJZSCX-02-11-24)资助.张贵仓,男,1964年生,博士,副教授,主要研究领域是计算机图形学、图像工程等. E-mail: zhanggc@nwnu.edu.cn.王让定,博士研究生,副教授,主要研究领域是数字水印技术、语音识别等.章毓晋,博士,教授,博士生导师,主要研究领域是图像工程(图像处理、图像分析、图像理解及其技术应用).

marking and other digital application areas.

Keywords digital image ; information hiding ; blending ; iteration ; digital watermarking

1 引言

随着 Internet 技术与多媒体技术的飞速发展, 数字化信息可以以不同的形式在网络上方便、快捷地传输. 数字信息与网络给人们带来方便的同时, 也给人们带来了隐患: 敏感信息可能轻易地被窃取、篡改、非法复制和传播等. 因此, 信息的安全与保密显得越来越重要, 信息安全已成为人们关注的焦点, 也是当今信息领域的研究热点之一^[1,2].

信息隐藏技术, 充分利用人们的“所见即所得”心理, 来迷惑恶意的攻击者, 即将信息隐藏于数字化媒体之中, 实现隐蔽传输、存储、标注、身份识别等功能. 由于图像比传统的文字蕴涵更大的信息量, 因而成为人们在信息利用方面的重要媒体, 图像隐藏也

成为研究的热点^[3~7]. 本文提出了一种基于迭代混合的数字图像隐藏方法, 可以有效地提高隐藏图像的安全性和抗攻击能力.

2 数字图像的混合

数字图像可以表示为连续函数在离散网格点处的函数值 $F_{i,j}$, 若其中 $i \in \{1, 2, \dots, M\}$, $j \in \{1, 2, \dots, N\}$, 那么, 这就是一个尺寸为 $M \times N$ 的图像.

定义 1. 若 F 与 G 分别表示尺寸为 $M \times N$ 的数字图像, α 为满足 $0 \leq \alpha \leq 1$ 的任一实数则称 S

$$S = \alpha F + (1 - \alpha) G \quad (1)$$

为数字图像 F 和 G 的 α 混合, 当参数为 0 或 1 时称为平凡混合. 为了叙述方便称 F 为载体图像, 称 G 为隐藏图像. 两幅图像的一个混合实例如图 1 所示.



图 1 图像的混合 ($\alpha=0.5$)

对于混合图像及被恢复的秘密隐藏图像我们可以采用均方根误差来反映他们的误差, 利用峰值信噪比来度量他们的客观保真度^[8]. 图像 F 和混合图像 S 的均方根误差为

$$RMSE = \left[\frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [F(i, j) - S(i, j)]^2 \right]^{\frac{1}{2}} \quad (2)$$

均方根误差越小, 说明两个图像越相似. 图像 F 和 S 的峰值信噪比 PSNR (Peak Signal-to-Noise Ratio) 为

$$PSNR = 10 \log_{10} \left[\frac{M \times N \times 255^2}{\sum_{i=1}^M \sum_{j=1}^N (F(i, j) - S(i, j))^2} \right] \quad (3)$$

峰值信噪比 PSNR 作为图像客观保真度准则, 它的值越大, 说明混合图像的保真度越好, 这两个图像越

相象.

根据混合图像的定义, 当混合参数 α 接近 1 时, 混合图像 S 就接近于图像 F , 当混合参数 α 接近 0 时, 混合图像 S 就接近于图像 G . 这样我们就可以利用人类视觉特性, 将一幅数字图像隐藏在另一幅数字图像之中, 将数字图像 F 和 G 做 α 混合: $S = \alpha F + (1 - \alpha) G$, 当混合参数 α 接近 1 时, 混合图像 S 就接近于图像 F , 可见的图像为 F , 图像 G 被隐藏, 隐藏的图像可用下面的公式恢复:

$$G = \frac{S - \alpha F}{1 - \alpha} \quad (4)$$

由于我们所处理的是数字图像, 在进行图像隐藏与恢复的计算过程中会产生误差, 误差与两幅图像及混合参数有关, 当两图像确定后误差仅与混合参数有关, 它是混合参数的函数, 如图 2 所示 (其中载体图像和隐藏图像分别为图 1 中的前两个图).

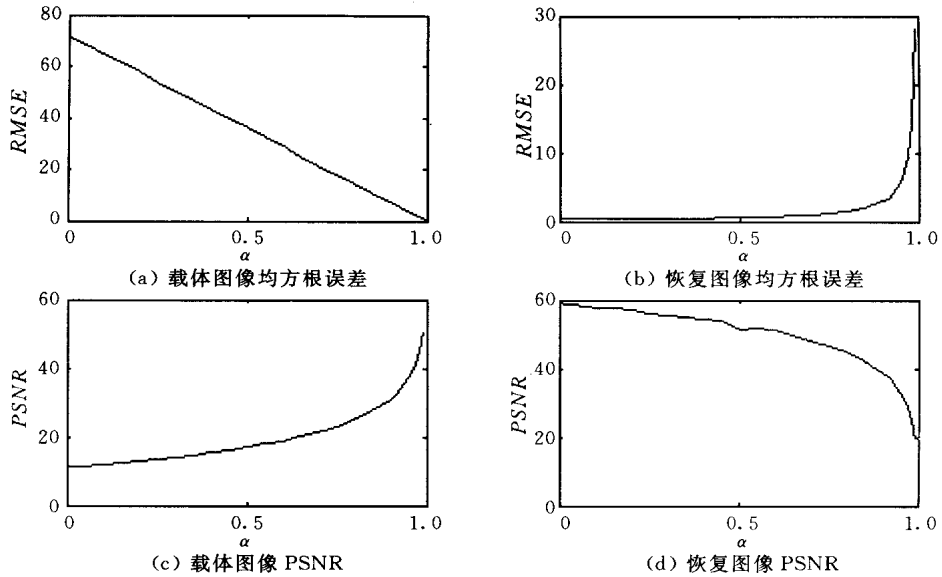


图 2 混合及恢复图像的质量与混合参数的关系

从图 2 中可以看到,当混合参数越接近 1,图像隐藏的效果就越好,而恢复图像的效果就差,恢复图像的误差增大;如果要求恢复的图像效果好,则混合参数就不能太接近 1,因此必须选择恰当的混合参数进行图像隐藏,事实上选取适当的混合参数,就可以得到很好的视觉隐藏与恢复效果,误差也是很小的,另外还存在最佳的混合隐藏,即混合图像与恢复图像误差和最小的图像混合,如图 3 曲线中的谷所示.

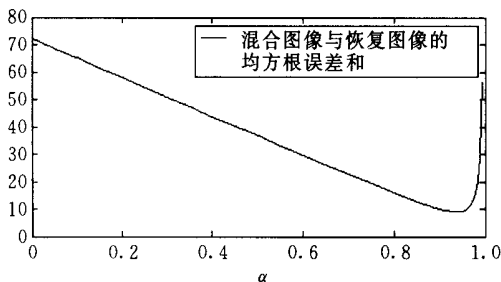


图 3 最佳混合曲线

综上所述,隐藏图像的一般性原则为:首先应选取与需要隐藏图像尽可能相像的载体图像,然后是在视觉允许的范围内选取尽可能小的混合参数,这样就可最大程度地保证恢复图像的质量.这种利用图像混合进行图像隐藏的方法,简便实用,然而混合参数的选取不太方便,为了克服这个缺点,我们提出了图像的迭代混合.

3 数字图像的单幅迭代混合

图像混合的核心是混合参数和混合图像,我们将它进行推广,利用多个参数进行多次混合,就有了

下面的迭代混合的概念.

定义 2. 设 F 与 G 分别表示尺寸为 $M \times N$ 的数字图像, $\{ \alpha_i | 0 \leq \alpha_i \leq 1, i = 1, 2, \dots, n \}$ 为给定的 n 个实数,对数字图像 F 和 G 进行 α_1 混合得 $S_1 = \alpha_1 F + (1 - \alpha_1) G$,将数字图像 F 和 S_1 进行 α_2 混合得 $S_2 = \alpha_2 F + (1 - \alpha_2) S_1$,依次进行混合得 $S_n = \alpha_n F + (1 - \alpha_n) S_{n-1}$,则数字图像 S_n 称为图像 F 和 G 的关于 α_i 的 n 重迭代混合.

定理 1. 数字图像 F 和 G 的关于 $\{ \alpha_i | 0 \leq \alpha_i \leq 1, i = 1, 2, \dots, n \}$ 的 n 重迭代混合图像 S 有

$$S = (\alpha_n + \alpha_{n-1} \alpha_n + \alpha_{n-2} \alpha_{n-1} + \dots + \alpha_1 \alpha_{n-1} \dots \alpha_2) F + \alpha_n \alpha_{n-1} \dots \alpha_2 \alpha_1 G \quad (5)$$

其中 $\alpha_i = (1 - \alpha_i), i = 1, 2, \dots, n$.

定理的证明是比较容易的,略去.

推论 1. 当 $\alpha_1 = \alpha_2 = \dots = \alpha_n = \alpha$ 时, $S = (1 - \alpha^n) F + \alpha^n G$, 其中 $\alpha = (1 - \alpha)$.

证明. 由式(7)有

$$\begin{aligned} S &= (\alpha_n + \alpha_{n-1} \alpha_n + \alpha_{n-2} \alpha_{n-1} + \dots + \alpha_1 \alpha_{n-1} \dots \alpha_2) F + \alpha_n \alpha_{n-1} \dots \alpha_2 \alpha_1 G \\ &= (\alpha + \alpha^2 + \dots + \alpha^n) F + \alpha^n G \\ &= (1 + \alpha + \alpha^2 + \dots + \alpha^{n-1}) F + \alpha^n G \\ &= \frac{1 - \alpha^n}{1 - \alpha} F + \alpha^n G \\ &= (1 - \alpha^n) F + \alpha^n G. \end{aligned}$$

定理 2. 数字图像 F 和 G 的关于 $\{ \alpha_i | 0 \leq \alpha_i \leq 1, i = 1, 2, \dots, n \}$ 的 n 重迭代混合图像 S_n , 当 $\alpha_i (i = 1, 2, \dots, n)$ 混合为非平凡混合时,混合图像 S_n 单调收敛于载体图像 F , 即有

$$\lim_{n \rightarrow \infty} S_n = F \quad (6)$$

证明. 由公式(5)就有

$$S_n = (\alpha_n + \alpha_{n-1} \alpha_n + \alpha_{n-2} \alpha_{n-1} + \dots + \alpha_1 \alpha_{n-1} \dots \alpha_2) F + \alpha_{n-1} \dots \alpha_2 \alpha_1 G \quad (7)$$

而

$$\begin{aligned} & \alpha_n + \alpha_{n-1} \alpha_n + \alpha_{n-2} \alpha_{n-1} + \dots + \alpha_1 \alpha_{n-1} \dots \alpha_2 + \alpha_{n-1} \dots \alpha_2 \alpha_1 \\ &= \alpha_n + \alpha_{n-1} \alpha_n + \alpha_{n-2} \alpha_{n-1} + \dots + \alpha_{n-1} \dots \alpha_2 + \\ & \quad \alpha_{n-1} \dots \alpha_2 (1 + \alpha_1) \\ &= \alpha_n + \alpha_{n-1} \alpha_n + \alpha_{n-2} \alpha_{n-1} + \dots + \alpha_{n-1} \dots \alpha_2 + \alpha_{n-1} \dots \alpha_2 \\ &= \dots = \alpha_n + \alpha_{n-1} = 1 \end{aligned}$$

故式(7)可写为

$$S_n = (1 - \alpha_{n-1} \dots \alpha_2 \alpha_1) F + \alpha_{n-1} \dots \alpha_2 \alpha_1 G \quad (8)$$

由于所有的混合都为非平凡混合,有 $0 < \alpha_i < 1$, $i=1,2, \dots, n$,因而也就有, $0 < \alpha_i < 1, i=1,2, \dots, n$,故有 $\alpha_{n-1} \dots \alpha_2 \alpha_1 > 0$,另外由于 $\alpha_{n-1} \dots \alpha_2 \alpha_1 < \alpha_{n-1} \dots \alpha_2 \dots \alpha_2 \alpha_1$ 则有 $(1 - \alpha_{n-1} \dots \alpha_2 \alpha_1) > (1 - \alpha_{n-1} \dots \alpha_2 \dots \alpha_2 \alpha_1)$,故迭代混合是单调的,由式(8)则定理得证.

由定理 2 就可得到一个自适应的图像隐藏方案.

隐藏算法 1.

Input $F, G, S = G$

Get a blending parameter $\alpha_1, 0 < \alpha_1 < 1$

$$\begin{aligned} \alpha_1 &= 1 - \alpha_1 \\ S &= \alpha_1 F + \alpha_1 S \end{aligned}$$

While $RMSE(S, F) > \delta$

Get a blending parameter $\alpha_i, 0 < \alpha_i < 1$

$$\begin{aligned} \alpha_i &= 1 - \alpha_i \\ S &= \alpha_i F + \alpha_i S \end{aligned}$$

End while

$$\alpha = \alpha_1 \alpha_2 \dots \alpha_n, \quad \alpha = 1 - \alpha$$

Output S .

注: δ 为控制迭代的参数.

秘密图像的恢复可使用公式(4)得到.

图 4 给出了利用迭代算法进行隐藏与恢复的例子,其中上排分别为迭代 1 次、2 次、3 次的混合图像,下排分别为从迭代混合图像中恢复的图像相关的数据,如表 1 所示.

表 1 单幅迭代混合实例相关参数

混合参数	混合图像 峰值信噪比	混合图像 均方根误差	恢复图像 峰值信噪比	恢复图像 均方根误差
0.8	24.9614	14.4036	45.1228	1.4138
0.7	35.4190	4.3211	34.5148	4.7951
0.6	43.3778	1.7284	26.3956	12.2112



图 4 单幅迭代混合隐藏实验

此外,我们对公开的混合图像也做了一些处理,包括增加污点、中心切除和不规则切除以考察算法的鲁棒性,从实验结果来看,算法还是具有一定的鲁棒性,如图 5 所示.

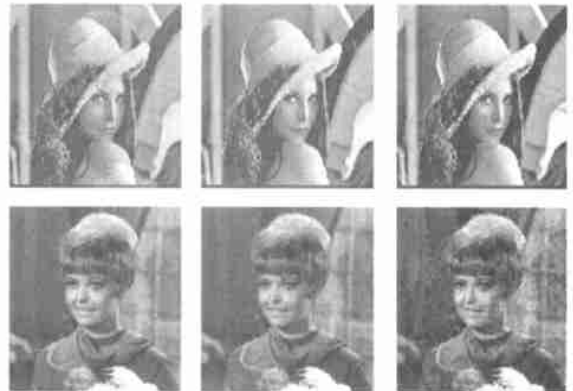


图 5 重迭代算法的鲁棒性实验 ($\alpha_1=0.8, \alpha_2=0.7, \alpha_3=0.6$)

4 数字图像的多幅迭代混合

上述图像混合算法及单幅迭代混合算法可以将一幅秘密图像隐藏在载体图像中,然而如果攻击者截获了载体图像和混合图像并产生了怀疑,则攻击者就完全有可能恢复出秘密图像,因此系统的安全性就完全依赖于载体图像的安全性上,这样的系统是脆弱的,为了解决这个问题,我们再将数字图像混合的思想推广,利用多个混合参数以及多幅图像来隐藏一幅图像,这就是数字图像的多幅迭代混合.

定义 3. 设 $F_i, i=1,2, \dots, n$ 和 G 分别表示尺寸为 $M \times N$ 的数字图像, $\{\alpha_i | 0 \leq \alpha_i \leq 1, i=1,2, \dots, n\}$ 为给定的 n 个实数,按照下面的方法做图像混合,对数字图像 F_1 和 G 进行 α_1 混合得 $S_1 = \alpha_1 F_1 + (1 - \alpha_1) G$,将数字图像 F_2 和 S_1 进行 α_2 混合得 $S_2 = \alpha_2 F_2 + (1 - \alpha_2) S_1$,依次进行混合得 $S_n = \alpha_n F_n + (1 - \alpha_n) S_{n-1}$,则数字图像 S_n 称为图像 G 的关于数字图像

组 $F_i, i=1, 2, \dots, n$ 的一个 n 幅迭代混合.

性质 1. 由定义 3 得到的混合图像满足下面的关系式.

$$S_n = \alpha_n F_n + \alpha_{n-1} F_{n-1} + \dots + \alpha_{n-1} \dots \alpha_{n-i+1} \alpha_{n-i} F_{n-i} + \dots + \alpha_1 F_1 + \alpha_2 F_2 + \dots + \alpha_n F_n \quad (9)$$

其中 $\alpha_i = (1 - \alpha_{i+1}), i=1, 2, \dots, n$.

由定义 3 就可直接得到式(8).

推论 2. 当 $\alpha_1 = \alpha_2 = \dots = \alpha_n = \alpha$ 时,有

$$S_n = (\alpha F_n + \alpha F_{n-1} + \dots + \alpha F_{n-i} + \dots + \alpha^{n-1} F_1) + \alpha^n G \quad (10)$$

其中 $\alpha = (1 - \alpha_{i+1})$.

根据数字图像多幅迭代混合的定义,我们就可以得到一个将一幅图像隐藏起来的方案,将需要隐藏的图像进行图像的多幅迭代混合,利用人类视觉的掩盖特性,将它隐藏在 n 幅图像中,隐藏和恢复算法如下.

隐藏算法 2.

```
Input G, alpha={alpha_1, alpha_2, ..., alpha_n}
S = G
For i = 1 to n do
Input F_i
```

```
Get blending parameter alpha_i
S = alpha_i * F_i + (1 - alpha_i) S
End for
```

Output S

恢复算法.

```
Input F, S, alpha={alpha_1, alpha_2, ..., alpha_n}
G = S
For i = n to 1 do
Input F_i
Get blending parameter alpha_i
G = (G - alpha_i F_i) / (1 - alpha_i)
End for
Output G
```

从恢复算法可以知道,隐藏图像的恢复必须依赖 n 幅混合图像、 n 个混合参数以及图像的混合次序,由此可见这种图像的多幅迭代隐藏方案是一种非常安全的隐藏方案,图 6 为多幅隐藏的例子,将 couple 混合在 girl 中,再混合到 lena 中,图 6 中的左图为多幅迭代混合后的公开图像,中间的图为将 couple 混合在 girl 中得到的中间过程图,右图为恢复出的隐藏图像.图 7 为多幅迭代混合隐藏算法的鲁棒性试验,其中对混合图像分别进行了增加污点、中心切除和不规则切除处理.



图 6 多幅图像隐藏($\alpha_1=0.9, \alpha_2=0.85$)



图 7 算法鲁棒性实验结果($\alpha_1=0.9, \alpha_2=0.8$)

我们还可以将图像的重迭代混合算法与多幅迭代混合算法组合起来,进行图像的隐藏,以进一步提高系统的安全性。

5 结 论

数字图像隐藏和数字水印是近年来新兴起的研究课题,本文利用图像的迷惑性和相关性得到了几个图像隐藏的算法,可以将一幅图像隐藏在一幅图像中。实验证明算法是可行的,隐藏和恢复图像的效果是良好的,算法还具有一定程度的鲁棒性,为了更进一步提高隐藏图像的健壮性和安全性,还可以将需要隐藏的图像进行置乱等预处理等^[7,9]。这种图像隐藏技术还可以推广到数字水印的研究中。

本文提出的迭代混合的思想仅仅是一个开始,基于图像混合的方法还有大量的工作可做,如隐藏算法的抗攻击性,恢复隐藏图像的鲁棒性以及鲁棒性的水印算法等^[10],希望本文能起到抛砖引玉的作用。

参 考 文 献

- 1 Bender W, Gruhl D, Morimoto N, Lu A. Techniques for data hiding. IBM System Journal, 1996, 35(3,4):313~335
- 2 Petitcolas F A G, Anderson R J, Kuhn M G. Information Hiding-A Survey. Proceedings of IEEE, 1999, 87(7):1062~1078
- 3 Su Zhong-Min, Lin Xing-Liang. The arbitrary share of visual secrets. Chinese Journal of Computers, 1996, 19(4):293~299 (in Chinese)



ZHANG Gu-Cang, born in 1964, Ph. D., associate professor. His research interests include mainly computer graphics, CAD, image engineering, digital watermarking.

WANG Rang-Ding, Ph. D. candidate, associate profes-

(苏中民,林行良.视图秘密的任意分存.计算机学报,1996,19(4):293~299)

- 4 Ding Wei, Qi Dong-Xu. Digital image transformation and information hiding and disguising technology. Chinese Journal of Computers, 1998, 21(9):838~843 (in Chinese)
(丁 玮,齐东旭.数字图像变换及信息隐藏与伪装技术.计算机学报,1998,21(9):838~843)
- 5 Wang Dao-Shun, Yang Lu. Visual hiding scheme using one secret image. Chinese Journal of Computers, 2000, 23(9):943~948 (in Chinese)
(王道顺,杨 路.图像的单幅可视隐藏方案.计算机学报,2000,23(9):943~948)
- 6 Wang Dao-Shun, Qi Dong-Xu. A new hiding scheme of digital image. Chinese Journal of Computers, 2000, 23(9):949~952 (in Chinese)
(王道顺,齐东旭.一种新的数字图像隐藏方案.计算机学报,2000,23(9):949~952)
- 7 Ding Wei, Yan Wei-Qi, Qi Dong-Xu. Digital image information hiding technology and its application based on scrambling and amalgamation. Journal of Image and Graphics, 2000, 5(8):644~649 (in Chinese)
(丁 玮,闫伟齐,齐东旭.基于置乱与混合的数字图像隐藏技术及其应用.中国图像图形学报,2000,5(8):644~649)
- 8 Zhang Yu-Jin. Image Engineering (1): Image Processing and Analysis. Beijing: Tsinghua University Press, 1999 (in Chinese)
(章毓晋.图像工程(上册)——图像处理和分析.北京:清华大学出版社,1999)
- 9 Qi Dong-Xu. Fractal and Its Generation by Computer. Beijing: Science Press, 1994 (in Chinese)
(齐东旭.分形及其计算机生成.北京:科学出版社,1994)
- 10 Zhang Gu-Cang, Zhang Yu-Jin. A new image-hiding scheme based on blending in DCT domain. Proceedings of SPIE, 2002, 4875:141~145

or,. His research interests include digital watermarking, and audio recognition.

ZHANG Yu-Jin, Ph. D., professor at Department of Electronic Engineering at Tsinghua University, Beijing, China. His research interests include mainly image processing, image analysis and image understanding, as well as their applications.