



1 概论

杨榆，钮心忻，周琳娜，雷敏

北京邮电大学信息安全中心

yangyu@bupt.edu.cn

提纲

- 隐写术和数字水印
- 隐写术和数字水印的历史
- 隐写术和数字水印的现状
- 信息隐藏的研究分支

典型隐写和数字水印系统

典型应用场景	干净的多媒体	藏有内容的多媒体	隐藏的内容
版权保护	作品	水印作品	水印
保密通信	载体	隐写对象	消息

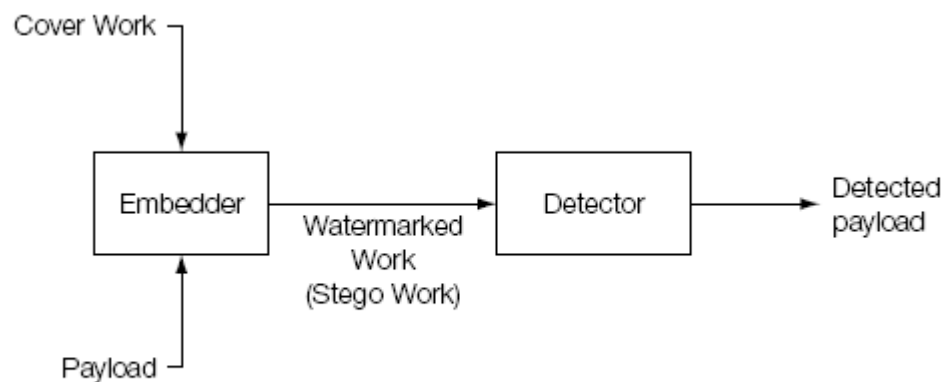


FIGURE 1.2

A generic watermarking (steganography) system.

图片源自 《Digital Watermarking and Steganography》

数字水印和隐写术

- 数字水印技术(Digital Watermarking)
 - 通过对媒体进行难以被感知的改动，从而嵌入与媒体有关的信息的技术。
- 隐写术(Steganography)
 - Steganography来自于希腊词根:steganos和graphie。

数字水印和隐写术

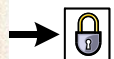
○ 隐写术(Steganography)

- Steganos指有遮盖物的;graphie指写。因此，Steganography的字面意思即为隐写。
- 隐写是通过对媒体进行难以被感知的改动，从而嵌入秘密信息的技术。

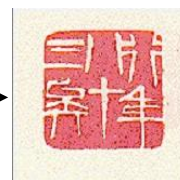
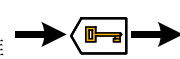
与密码技术的区别

Alice

Bob



釘廬?a懷嶠?默 禄`往? r,拈,?\$ }!
鍍?\YM}q 銅 J?无T 欣歆YB8既\$町 々P?k蒔
PRd敗:*/I却媼傘弥蔞頰 ?::?8拚?t〃霹諄
R2MrK?嶼F6 v[越穗2??掘瓊橫 販 3;iu轆 ?
堦` ? 詠っ昕?欽L鯨剛危?8脂g游 裏L!准
%s?鈔K%既~1鱣(肱T掩+擧<?迹N帝4 g \??辰
+t嘆I 貽洩鸚惇 凝?\ e8T/1E孺s ? .?e/
1睛<消`圣'\矜杆J 卜1煇 壘? SC 9



与密码技术的区别



与密码技术的区别

在公开信道中传输的信息的形态不同



Rar!000嫩s00
0000000P岭 侄00000#0000}吓ef?503\$0 000新建 文本文档.txt0ea苞^ 嚇,g囁h.0tx
?
?0z漲潯婁a?0000L?7`fK0?:0艷B飾0睨fGC?糾蓉氧,x姜??鞞!4ry鑰偵鱗???蘇0M,0000:
鵠#?'行订?u叛A9s%偉K燕#of?0緬鰓?0鉞嗽?b氷煸b0s0?8項瓊?0汀T和
??0岷Z ?哽= ?0
{R00y~T摺飯I}^_b嚟枯0簪 汙?d? 瘕?祥?鵠?{0000

乱码

“普通”数字媒体（调制）

与密码技术的区别

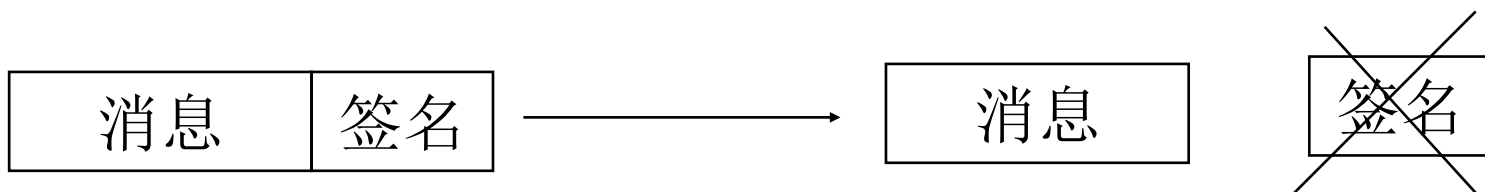
抗干扰能力不同

Rar!0000s00
0000000P冷 促00000#0000}吓€f?503\$0 000新建 文本文档.txt0ea苞^ 嚇,g單h.0tx
?
?0z振潏婁a?0000L?7`fKO?:0艷B誦0脫fGC?紹|荖氧 x姜??賴'4ry鑰倡轄??薛0M,0000:
鵠#?'行订?u叛A9s%偉K莖#of?0緬臨?0鉞嗽?b氷梯b0s0?8頂璩?0打T和
??0岨Z ?哽= ?0
(ROOy~T習飯I)^_b嚙枯0簪 汙?d? 癩?祥?鵠?(0000



与密码技术的区别

抗“剥离”能力不同



无法剥离

与密码技术的区别

○ 密码学

- 密文是不可懂的“乱码”
- 不容错
- 签名可剥离
- 秘密信息不可懂

○ 信息隐藏

- 载体对象和隐写/水印对象类似
- 误码不扩散
- 水印不可去除
- 秘密信息不可见

提纲

- 隐写术和数字水印
- 隐写术和数字水印的历史
- 隐写术和数字水印的现状
- 信息隐藏的研究分支

信息隐藏的历史

- 古典广义信息隐藏技术
 - 技术型
 - 语言学型
 - 版权保护型

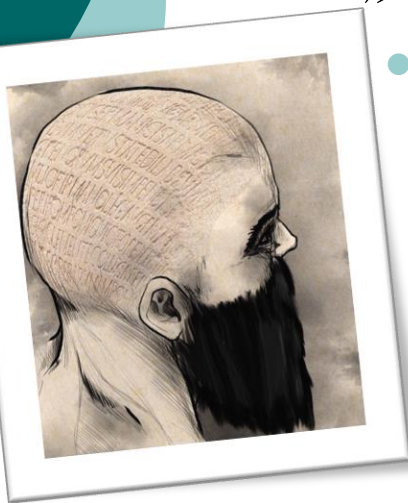
隐写术和数字水印历史——技术型技术

○ 历史记载的最早应用

- 希腊历史学家希罗多德（Herodotus）描述的一段公元480年前的历史。希斯提乌斯(Histiaeus)想给希腊城邦米利都（Miletus）的摄政者传递消息，鼓动他们反抗波斯占领者。希斯提乌斯想出了一个巧妙、但很缓慢的安全通信方法，剃了头的奴隶，把消息纹在头皮上，等头发长出后，派遣到米利都。在那里，再次剃光奴隶的头发，便获取秘密消息。

○ 书记板的故事

- 德莫瑞特思通过书记板提醒了斯巴达(Sparta)，告知了波斯国王薛西斯(Xerxes)入侵希腊的计划。他首先去掉书记板上的蜡，然后将消息写在木板上，再用蜡覆盖，这样处理后的书记板看起来是一个完全空白的。



隐写术和数字水印历史——技术型技术

○ 实物隐藏

- 将信函隐藏在信使的鞋底、衣服的皱褶中，妇女的头饰和首饰中等。

○ 标记法

- 刺孔、字母高度、笔画粗细
- 在一篇信函中，通过改变其中某些字母笔划的高度，或者在某些字母上面或下面挖出非常小的孔，以标识某些特殊的字母，这些特殊的字母组成秘密信息。

隐写术和数字水印历史——技术型技术

○ 显影剂

- 隐形墨水：碘和淀粉、米汤和烟。。。。
- 化学的进步促使人们开发更加先进的墨水和显影剂
- 但随着“万用显影剂”的发明，此方法就无效了。
 - 其原理是，根据纸张纤维的变化情况，来确定纸张的哪些部位被水打湿过，这样，所有采用墨水的隐写方法，在“万用显影剂”下都无效了。

隐写术和数字水印历史——技术型技术

- 微缩胶片 (Digital Watermarking and Steganography)
 - Another idea that played an important role in several wars in the nineteenth and twentieth centuries was originally proposed by Brewster (1857) .
 - He suggested hiding messages by shrinking them so much that they started resembling specs of dirt.

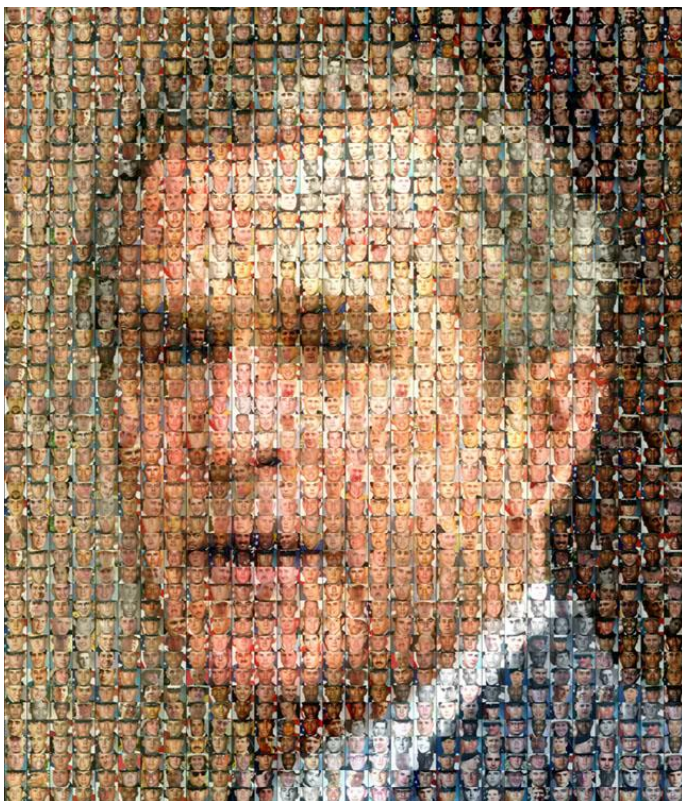
隐写术和数字水印历史——技术型技术

- 微缩胶片 (Digital Watermarking and Steganography)
 - The shrinking was made possible by the technology developed by French photographer Dragon during the Franco-Prussian War (1870–1871).
 - Microscopic images could be hidden in nostrils, ears, or under fingernails.

隐写术和数字水印历史——技术型技术

- 微缩胶片 (Digital Watermarking and Steganography)
 - In World War I, Germans used such “microdots” and hid them in corners of postcards slit open with a knife and resealed with starch.
 - The modern twentieth-century microdots could hold up to one page of text and even contain photographs. The Allies discovered the use of microdots in 1941.

隐写术和数字水印历史——技术型技术



○ 微缩胶片

- 主要思想：缩拍图片。
- 左图展示其宏观效果。
- 小布什头像由若干士兵头像组成。

隐写术和数字水印历史——技术型技术

摩斯码 (Digital Watermarking and Steganography)

- A more recent and quite ingenious use of steganography helped Commander Jeremiah Denton convey the truth about his North Vietnamese captors.
- When paraded in front of the news media as part of staged propaganda, Denton blinked his eyes in Morse code spelling out T-O-R-T-U-R-E.

隐写术和数字水印历史——技术型技术

摩斯码 (Digital Watermarking and Steganography)

- 谷歌和Genius.com的歌词之争
- <https://www.pcmag.com/news/369096/google-we-dont-scrape-websites-for-song-lyrics>

Not Today

Alessia Cara

Someday I won't be afraid of my head
Someday I will not be chained to my bed
Someday I'll forget the day he left
But surely not today
One day I won't need a PhD
To sit me down and tell me what it all means
Maybe one day it'll be a breeze, ah
But surely not today, but surely not today

Oh, you don't know what sadness means
Til you're too sad to fall asleep
One day I'll be snoozing peacefully
But surely not today, surely not today

One day I'll swear the pain will be a blip
I'll have the hardest time recalling it
I'll be the king of misery management
But surely not today

Google issued the denial after Genius.com said it had proof the lyrics copying was taking place. In 2016, the music website began watermarking certain song lyrics using patterns of apostrophes to spell out the word "Red-handed" when translated in Morse code.

According to *The Wall Street Journal*, the music website has found more than 100 examples of Google's search engine taking its lyrics and displaying them over "information panels," which will appear as the top result on song lookups.

隐写术和数字水印历史

——语言学型技术

○ 藏头诗

○ 平湖一色万顷秋，

○ 湖光渺渺水长流。

○ 秋月圆圆世间少，

○ 月好四时最宜秋。

○ 芦花丛中一扁舟，

○ 俊杰俄从此地游。

○ 义士若能知此理，

○ 反躬难逃可无忧。

隐写术和数字水印历史

——语言学型技术

President's embargo ruling should have immediate notice. Grave situation affecting international law. Statement foreshadows ruin of many neutrals. Yellow journals unifying national excitement immensely.

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Pershing sails from NY June 1

隐写术和数字水印历史

——语言学型技术

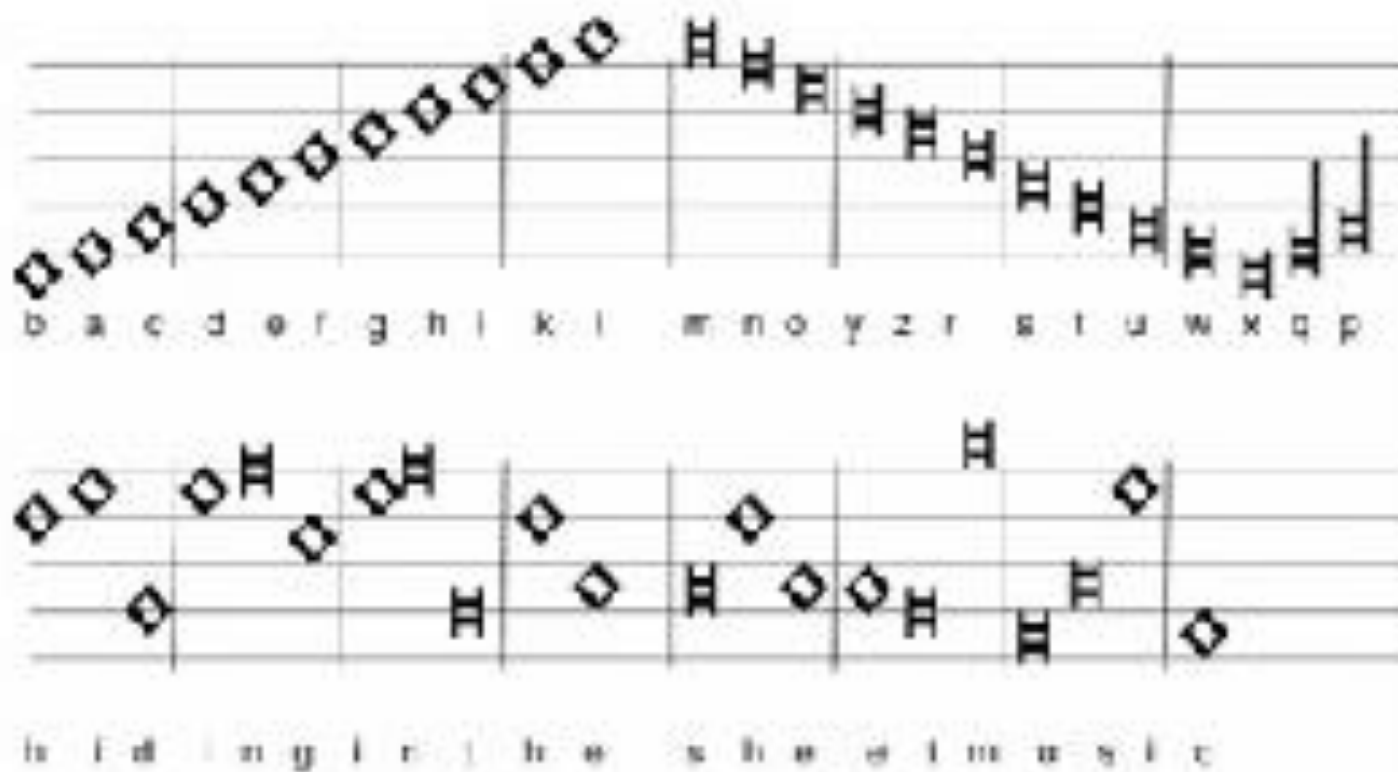
○ 卡登格子

- 中国古代设计的信息隐藏方法中，发送者和接收者各持一张完全相同的、带有许多小孔的纸，这些孔的位置是被随机选定的。发送者将这张带有孔的纸覆盖在一张纸上，将秘密信息写在小孔的位置上，然后移去上面的纸，根据下面的纸上留下的字和空余位置，编写一段普通的文章。接收者只要把带孔的纸覆盖在这段普通文字上，就可以读出留在小孔中的秘密信息
- 在16世纪早期，意大利数学家Cardan(1501-1576)也发明了这种方法，这种方法现在被称作卡登格子法

隐写术和数字水印历史

——语言学型技术

○ 乐谱法

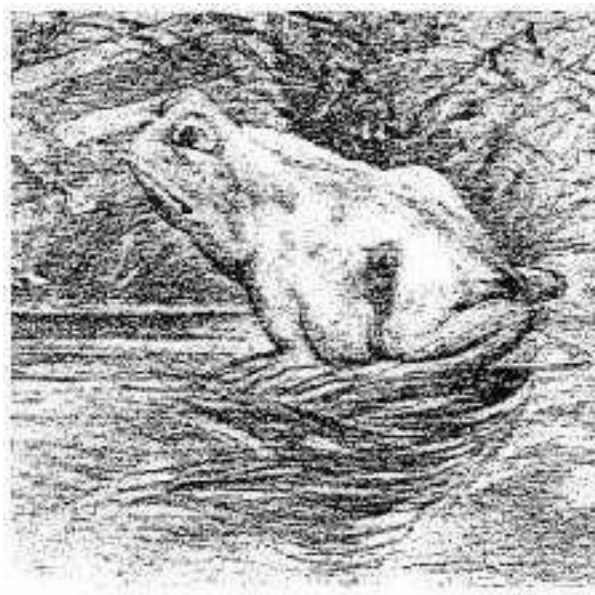


隐写术和数字水印历史

——艺术作品中的隐写术

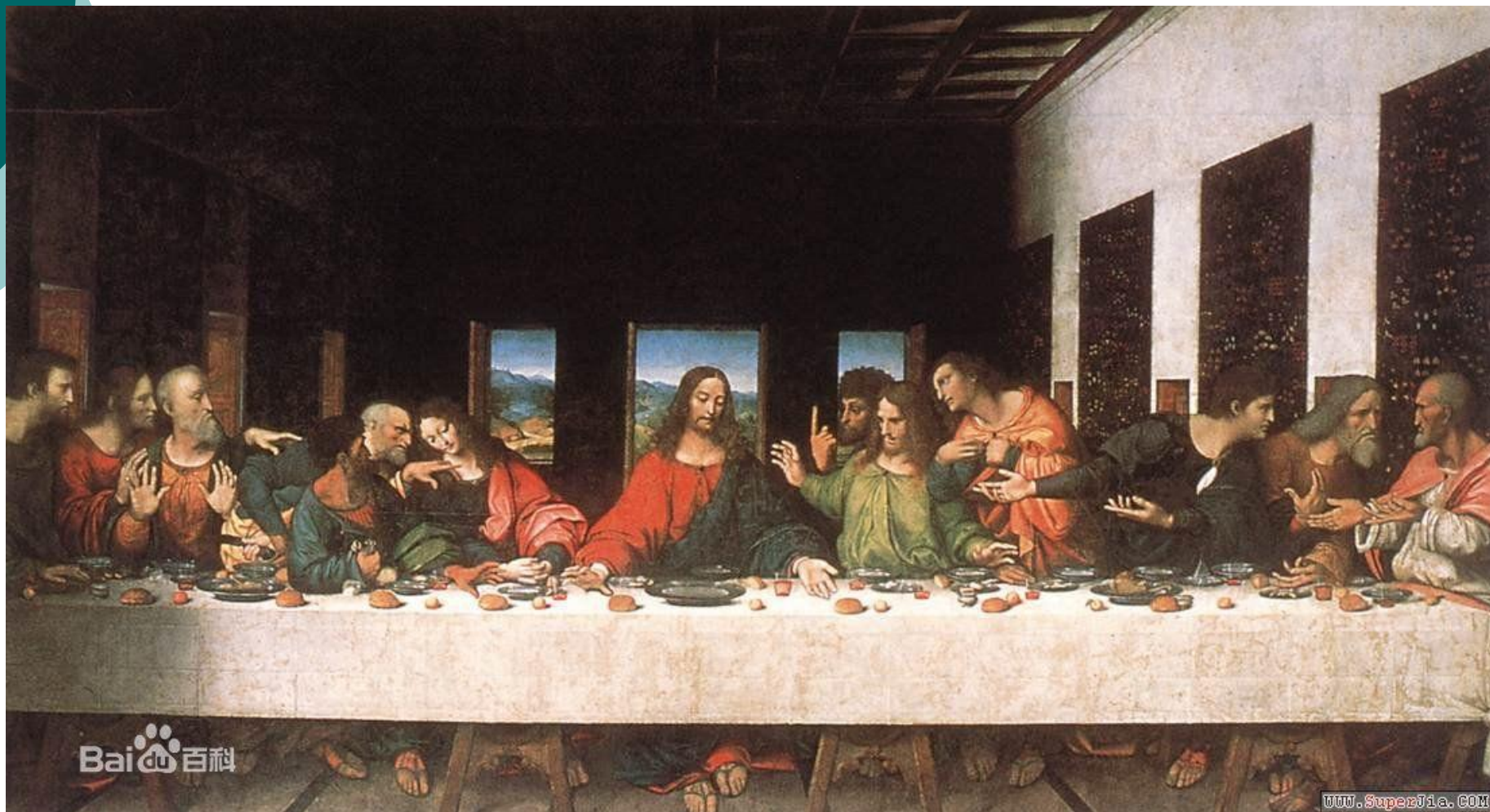
○ 在艺术作品中的隐写术

- 在一些变形夸张的绘画作品中，从正面看是一种景象，侧面看又是另一种景象，这其中就可以隐含作者的一些政治主张或异教思想



隐写术和数字水印历史

——艺术作品中的隐写术



隐写术和数字水印历史

——版权保护



○ 核对校验图（作品的摘要）

- Lorrain(1600-1682)是17世纪一个很有名的风景画家，当时出现了很多对他的画的模仿和冒充，由于当时还没有相关的版权保护的律，他就使用了一种方法来保护他的画的版权
- 他自己创作了一本称为《**Liber Veritatis**》的书，这是一本写生形式的素描集。他创作这本书的目的是为了保护自己的画免遭伪造。一个细心的观察者根据这本书仔细对照后就能判定一幅给定的油画是不是赝品

隐写术和数字水印历史

——版权保护型技术

○ 纸张中的水印

- 水印是从特定角度观察时才显现的纸张上的图案，主要用于防伪。
- 在造纸过程中，使用模具改变纸浆密度而形成的图案，称为水印。因为印记是在纸浆还在水中时制作的，故而称为水印。

隐写术和数字水印历史

——版权保护型技术

随着技术的进展，人们可以在纸张中加入水印。一些高级酒店成为首批使用者之一。这些酒店会提含有酒店标识的信签纸，彰显酒店的服务和档次。

作为高档酒店的标识，水印也出现在了这类酒店的信纸中。添加水印并不是为了保护版权，而是为了宣传和展示。

隐写术和数字水印历史

——版权保护型技术

固定头像水印：

- 纸币中的水印
 - 演示，纸币中

位于票面正面左侧空白处，迎光透视，可见与主景图像相同、立体感很强的毛泽东头像水印。



隐写术和数字水印历史

——版权保护型技术

- 纸币中的水印

- 演示，纸币中

白水印：

位于正面双色异形横号码下方，迎光透视，可以看到透光性很强的水印“100”字样。



隐写术和数字水印历史——小结

- 古典隐写术和水印技术
 - 丰富想象力
- 现代隐写术和数字水印技术
 - 数字信号处理、编码技术、统计分析...
 - 感知系统的冗余

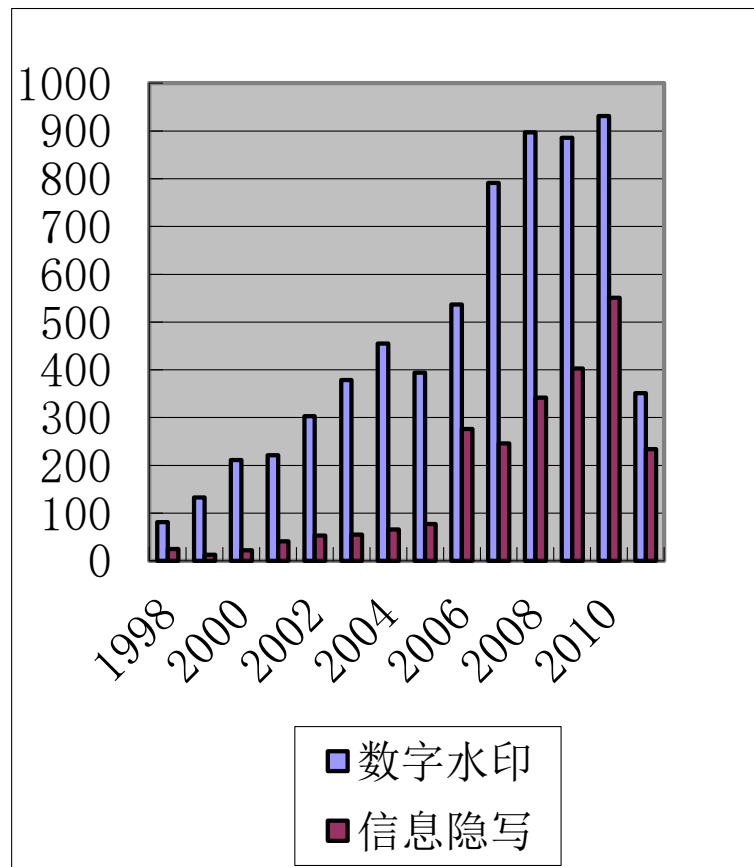
提纲

- 隐写术和数字水印
- 隐写术和数字水印的历史
- 隐写术和数字水印的现状
- 信息隐藏的研究分支

信息隐藏发展阶段

20世纪90年代开始迅速发展

- 1988年，Komatsu和Tominaga，首次使用“数字水印”这一术语。
- 1992年国际上正式提出信息隐形研究。
- 1995年数字水印相关文献大量涌现。
- 1996年国际第一届信息隐藏研讨会(IHW)。
- 1999年中国第一届信息隐藏研讨会(CIHW)。



信息隐藏发展阶段

- 90年代，多个组织开始考虑将数字水印技术纳入标准
 - The Copy Protection Technical Working Group (CPTWG)
 - The Secure Digital Music Initiative (SDMI)
 - Two projects sponsored by the European Union, VIVA and Talisman
 - The International Organization for Standardization (ISO)

信息隐藏发展阶段

- 90年代后期，一些公司推出了水印产品
 - SDMI采用了Verance Corporation的水印技术用于互联网音频分发保护，例如Liquid音频
 - Digimarc绑定水印嵌入和提取器到Adobe产品Phtoshop

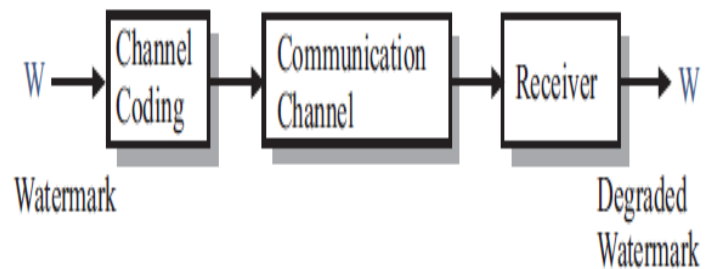
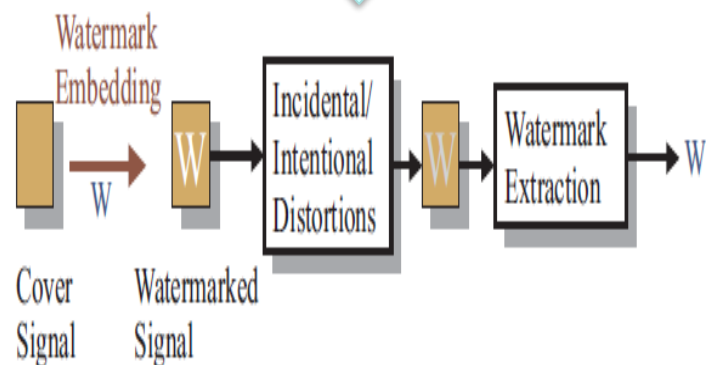
信息隐藏发展阶段

把信息的隐藏和提取视作一个通信问题，用通信理论解决容量分析等问题

理论研究的热潮（2000年后）

Moulin等人提出基于信息论的信息隐藏理论框架

- Costa dirty paper 模型
- Cohen与Lapidoth模型
- Somekh-Baruck模型
- 并行高斯信道模型等
- 这些模型的共同点都是把信息隐藏类比于一个通信模型，其差别在于对攻击行为及信道的描述或假设不同
- 信息隐藏的容量被认为是上述通信模型下最大可靠传输率



隐写术和数字水印现状

○ 产品、软件

- MP3Stego
- Jstego
- Stools(wav,gif,bmp)
- OutGuess
- ...

○ 产品、软件

- <http://www.jjtc.com/Steganography/toolmatrix.htm>
- 信息隐藏主页
(petitcolas维护)
<https://www.petitcolas.net/steganography/>

隐写术和数字水印现状

ALPHA TEC LTD™ GRAPHICS, COMPUTER VISION, SIGNAL AND IMAGE PROCESSING AND ANALYSIS SOFTWARE

Search this site **GO!**
Search help & tips

General
[Home](#)
[All Products](#)
[Order form](#)

Products
[Image Processing](#)
[3D Imaging](#)
[Digital Video](#)
[MPEG-7](#)
[Dentistry/Medicine](#)
[Museum Apps](#)
[Watermarking](#)
[Banking Applications](#)
[Maya plugins](#)
[3D Terrain visualization](#)

Alpha Tec Ltd
is a company specialized in digital image/video processing and multimedia in a multitude of applications.

[More Info](#)

EIKONA3D
EIKONA3D for Windows is an integrated, powerful and flexible software package for 3D image processing, analysis and visualization.

[More Info](#)
[Try It!](#)

EIKONAMARK
Eikonamark is a software for casting "invisible" watermarks (signatures) on digital images and detecting these watermarks.

[More Info](#)
[Try It!](#)
[Buy It!](#)

Find a product
Select from the list:

Newsletter sign-up
Get the latest news about our products by email!
 type your e-mail
SUBMIT

Solutions for:

- Digital artists
- Photographers
- Museums
- 3D model designers

Find out how to protect your:

- Digital images
- Digital audio
- Digital video
- Vector graphics
- 3D mesh objects

Latest news:


- » **NEW! EIKONA Subtraction Radiography** [Try It!](#)
- » AlphaGeo: 3D terrain visualization application! [Try It!](#)
- » VIDEO MARK SDK: Video watermarking library! [Try It!](#)
- » DIVA3D Library! Powerful video processing library! [Try It!](#)


AlphaGeo **NEW**
AlphaGeo enables Internet Explorer to

隐写术和数字水印现状

A screenshot of the Blue Spike website. The header features the 'BLUESPIKE' logo in a stylized blue font, followed by navigation links: '| Art | Science | Technology | Company | Contact Us |'. Below the header is a large banner image with a blue and white bar chart and abstract line patterns. The main text on the banner reads 'Blue Spike®: Innovations in Copyright Management & Applied Security'. Below this, a paragraph states: 'With over 49 patents ranging from forensic watermarking to content management, Blue Spike has established itself as the leading provider of applied security solutions.' A second row of navigation links follows: '| About | Patents | Management | Advisors | Partners | Investor Relations | Career Opportunities |'. The page is divided into two columns. The left column is titled 'What is Digital Watermarking?' and contains the text: 'Digital watermarking is a process of encoding information into a data stream, so as not to impact the overall composition; but, enables identifying, verifying and'. The right column is titled 'Giovanni® Digital Watermarking Suite' and contains the text: 'With Giovanni, digital information can be securely labeled, audited, and even used to animate automated marketing and consumer interaction under a wide number of deployments.' At the bottom of the right column are links: '| Overview | Process | Specs | FAQ |'.


隐写术和数字水印现状

DIGIMARC | 

[DIGIMARC DISCOVER](#) | [DIGIMARC FOR IMAGES](#) | [DIGIMARC CORPORATE](#) | [INVESTORS](#) | [SEARCH](#) 

DIGIMARC DISCOVER™

Enable your phone to “see and hear” with Digimarc Discover; recognize all forms of media in your surroundings to enrich and simplify your life.

DIGIMARC | 
discover

OPEN BETA | [LEARN MORE](#)

for publishing

for music

for packaging

for movies & TV

隐写术和数字水印现状

○ 促因

- 版权保护

- 1999年，专栏作家诉纽约时报等4家媒体

- 1999年，王蒙等诉网站擅自在网上传播其作品

○ 促因

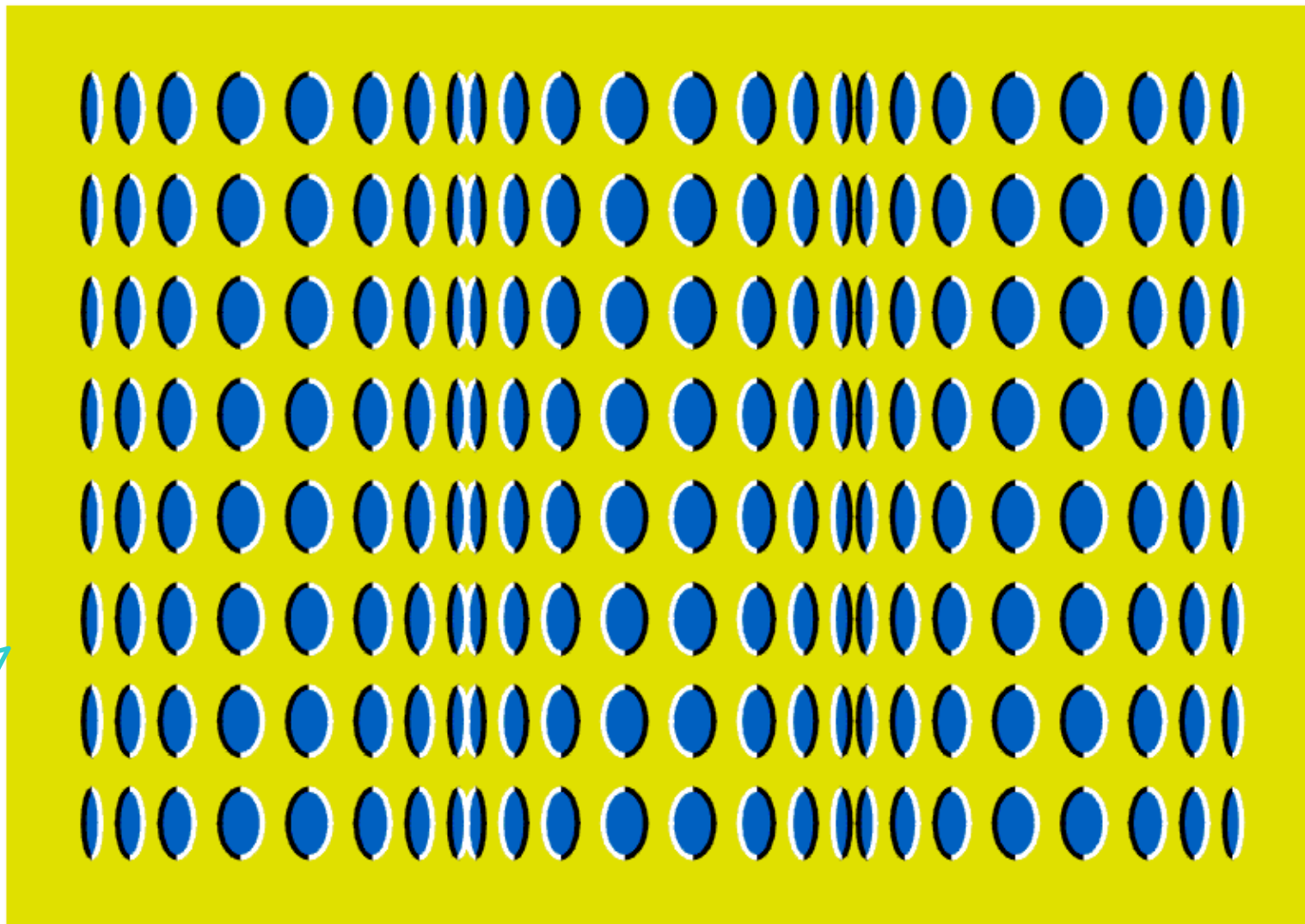
- 保密通信

- 2001年，9.11



隐写术和数字水印现状

C

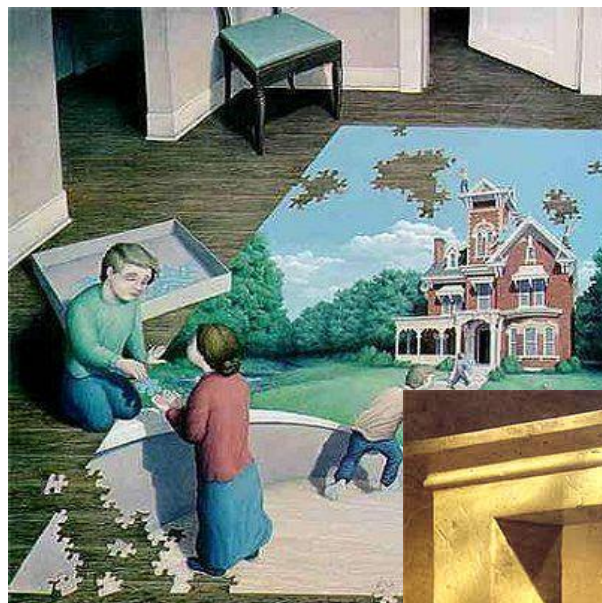


感知心理学研究表明：一个人承受的压力越大，注意力越分散，画面转速越大！

隐写术和数字水印现状

○ 保障

- 信号处理技术发展
- 人类感知系统的冗余（生理学、心理学）
- 海量的信息



隐写术和数字水印现状

——研究课题

○ 正向研究

- 基于图像的隐写和数字水印技术较成熟
- 基于音频的隐写和数字水印技术还在发展
- 视频隐写和数字水印的研究是新兴的热点
- 文本、协议、软件...
- 信息隐藏在物联网、大数据隐私保护、区块链等新场景的应用。

隐写术和数字水印现状

——研究课题

逆向研究

- 主动攻击：在不显著影响使用价值前提下，尽量抹除信息。
- 被动攻击：判定并提取待检测载体中信息

○ 新研究点

- **Benchmark (Stirmark)**，数字图像取证，感知哈希。

○ 理论研究

- 容量研究（博弈法、信息论法）

隐写术和数字水印现状

——研究层次

应用技术研究

以实用化为主要目的，研究各种多媒体格式的数字水印在实际中的应用

应用基础研究

针对图像、声音、视频等载体，研究相应的数字水印隐藏算法和检测算法

基础理论研究

信息隐藏模型、理论框架、容量、安全性理论等

隐写术和数字水印现状

——文献检索（关键词）

- Information Hiding（信息隐藏）
- Steganography（隐写）
- Steganalysis（隐写分析）
- Digital Watermarking（数字水印）

提纲

- 隐写术和数字水印
- 隐写术和数字水印的历史
- 隐写术和数字水印的现状
- 信息隐藏的研究分支

信息隐藏研究分支

- 隐写术—伪装式保密通信
- 数字水印—数字产品版权保护
- 隐蔽信道—计算机系统中的一些通道
- 信息分存—可视密码
- 数字图像取证—真实性鉴别

信息隐藏研究分支——隐写术

- 利用人类感知系统以及计算机处理系统的冗余隐藏信息。
- 载体可以是任何一种多媒体数据，如音频、视频、图像、甚至文本、数据等。
- 被隐藏的信息也可以的任何形式。
- 主要用于军队和安全部门。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 广播监控(Broadcast Monitoring)

- 1997年，日本发生电视广告丑闻。至少有两家电台没有播出部份已付费的广告节目。这样的情况已持续超过20年而没有被发现，重要原因之一是没有系统监控实际播出的广告内容。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 广播监控(Broadcast Monitoring)

- 1999年，美国演员协会调查发现，平均而言，美国每小时广播节目少付了**1000**美元版税。
- 此外，版权所有者还关心，广播的作品究竟是正版还是盗版作品。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 广播监控(Broadcast Monitoring)

- 有多家公司提供了基于水印技术的广播监控服务，例如，Teltrax提供了基于Philips视频水印技术的广播监控。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 版权保护(Copyright Protection)

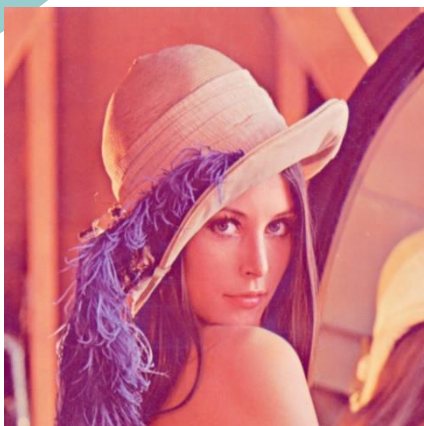
- 早期版权保护方式存在漏洞，只有在作品中能发现版权申明时，版权所有者才能获相关补偿。然而，这种在作品某个部份增加的的申明很容易被去除。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 版权保护(Copyright Protection)

- 常用测试图像Lena实际属于某杂志。
- 最早使用该图像的研究者扫描时，只保留了Lena的脸部和肩部，遗漏了杂志的版权申明，以致于全世界大部份相关论文都使用了该测试图像而不知侵犯了该杂志的版权。



信息隐藏研究分支——数字水印

○ 数字水印应用

● 版权保护(Copyright Protection)

- 最终该杂志决定忽略对该图像的“侵权”使用。
- 水印具有不可感知性、不可分离性，因此既能有效提供媒体的版权所有者身份证明，又不会降低媒体感官效果。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 版权保护(Copyright Protection)

- Digimarc公司的图像水印是典型范例。
- Digimarc的图像水印检测器与Adobe图像处理软件Photoshop捆绑发布，一旦Digimarc的图像水印检测器发现水印，就通过水印信息检索互联网数据库，获取作者联系方式。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 盗版追踪(Transaction Tracking)

- 在每份正版作品中嵌入唯一标识（指纹）后，一旦出现盗版，就可以追踪其来源。
- 2004, 使用Philips视频水印技术嵌入“指纹”信息的预览片被分发给5803名奥斯卡观影评选员，供评选员观看评分。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 盗版追踪(Transaction Tracking)

- 后来，其中一部影片的视频出现在互联网。分析这些盗版视频发现其源自一位观影评选员的拷贝。该评选员曾把其拷贝提供给他的朋友。虽然他不知道自己朋友的作为，但这位**70**岁的演员仍然被起诉，罚款**300**万美元。

信息隐藏研究分支——数字水印

数字水印应用

- 盗版追踪

- 《画皮2》 2012年上映不久便被盗版，华谊兄弟根据相关的水印信息分析，确认出视频的盗版源。



信息隐藏研究分支——数字水印

○ 数字水印应用

● 内容认证(Content Authentication)

- 数字媒体能够被轻易篡改。密码学提供了认证方式，对媒体签名。
- 签名通常存放在文件头或特定结构中，一旦格式变换，签名可能丢失。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 内容认证(Content Authentication)

- 脆弱水印思路之一是将签名嵌入媒体，例如，媒体的高比特平面产生签名，低比特平面承载水印。图像的任何改动都能被判别出。
- 半脆弱水印能够容忍常规图像处理操作，例如格式转换，去噪，并检测定位内容篡改操作。
- 水印还可用于图像的修复和还原。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 拷贝控制(copy control)

- 一种方式是加密。例如电视信号加密传输，只有包含特定密钥的机顶盒能够解密信号。这种方式的问题是，解密后的电视信号可以输出并被录制、刻录。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 拷贝控制(copy control)

- 另一种思路是每个刻录装置都配有水印检测设备，一旦检测到“禁止刻录”水印，便停止刻录。
- CPTWG(Copy Protection Technical Working Group)，和SDMI(Secure Digital Music Initiative)分别提出用于视频和音频的系统构想。

信息隐藏研究分支——数字水印

○ 数字水印应用

● 设备控制(device control)

- 拷贝控制实际设备控制的一种。设备控制更多地是丰富，而不是限制对媒体的使用。
- 例如Digimarc的媒体桥技术。
- 杂志中的广告画面包含水印，使用手机捕获画面后，手机软件识别水印信息，并导航到相关网站。

信息隐藏研究分支——数字水印

○ Digimarc MediaBridge

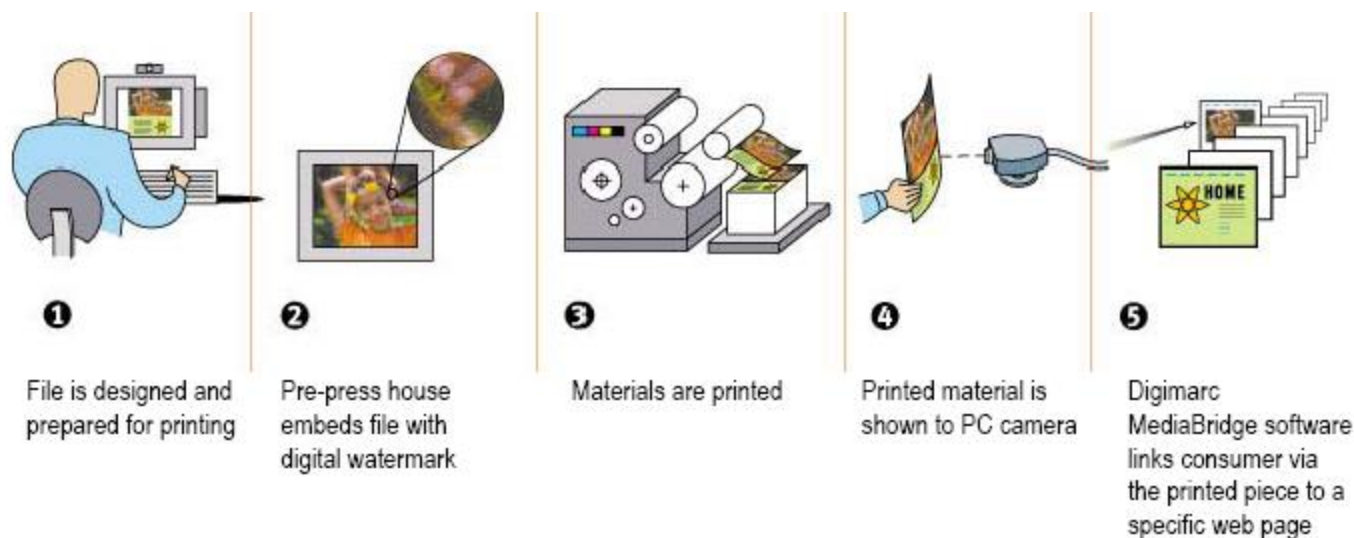


Figure 1 : Digimarc MediaBridge Process Flow

图片源自: Burt Perry, Brian MacIntosh, Dave Cushman. Digimarc MediaBridge - The Birth of a Consumer Product, from Concept to Commercial Application.

信息

数字



Calculator



Digimarc



玩校App



北京邮电大学



2024/11/6

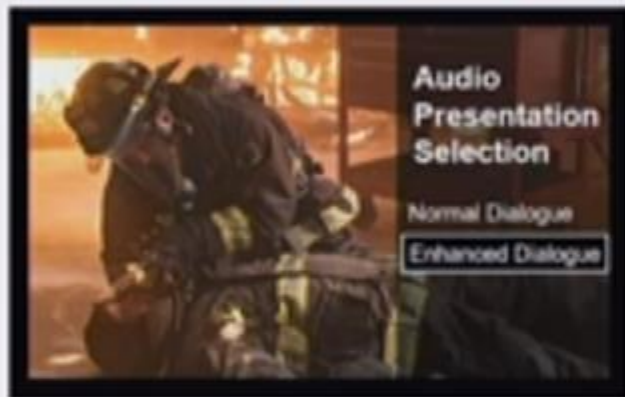
信息隐藏与数字水印

信息隐藏研究分支——数字水印

Personalized Audio

Enabled by the Aspect Watermark and Dolby AC-4 Next Gen Codec

Dialogue Enhancement



Brings dialogue forward relative to background noise

Audio Replacement



Select from multiple languages or Visual Description Services

Alternative Commentary



Select audio commentary from alternate sources



verance.com

© 2013 Verance Corporation, Google

分支——数字水印

- 数字水印应用

- 标注(captioning)

- 网络多媒体资源（音频、图像、视频...）中嵌入信息（标题、关键词、分类...），便于多媒体检索。
 - 把感兴趣的图像特征（或区域）的位置和识别信息嵌入图像中，可以实现特征定位和识别。

分支——数字水印

○ 数据泄露溯源

- 在数据库对数据进行脱敏时，将标识信息与隐私保护算法或参数关联，使得脱敏后的数据自身就携带了标识信息。
- 一旦发生数据泄露，通过泄露的数据样本，便能一定程度上追溯泄漏源。
- 腾讯云采用这种方法应对数据泄露风险。

分支——数字水印

○ 数据泄露溯源

- 另一种方法并不修改原始数据样本，而是插入符合原始数据样本统计特征的“假”记录。
- 若数据泄露，则“假”记录也会一并泄露。在暗网、**Dropbox**等市场检测假记录的有无，就能及时掌握数据泄露状况。
- 进一步地，假记录还具有“蜜罐”效果，检测假记录配对邮箱的异常邮件信息，可以得到竞争对手等记录购买者信息。
- 此类公司的代表有**Bitglass**，**DigitalShadow**，**RepKnight**等。

分支——隐蔽信道

○ 隐蔽信道

- 隐蔽信道是相对于公开信道而言的，和公开信道一起使用，公开信道上传输的信息，是隐蔽信道的载体，
- 例如：**TCP**协议头中保留字段可用于携带秘密信息。

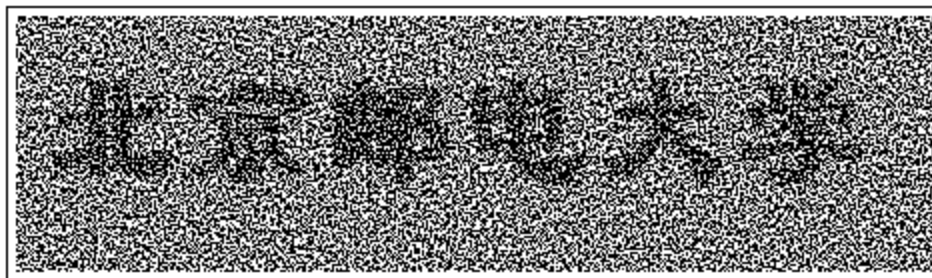
源端口:8bit										目的端口:8bit									
序号:32bit																			
确认序号:32bit																			
协议头 长度:4bit		预留:6bit				U	A	P	R	S	F	窗口大小:16bit							
						R	C	S	S	Y	I								
						G	K	H	T	N	N								
校验和:16bit												紧急指针:16bit							
选项												填充							
数据																			

信息隐藏研究分支——可视密码

- 1994年，M.Naor和A.Shamir提出。
- 其思想是把要隐藏的密钥信息通过算法隐藏到两个或多个子密钥图片中。
- 每一张图片上都有随机分布的黑点和白点。
- 把所有的图片叠加在一起，则能恢复出原有的信息。

信息隐藏研究分支——可视密码

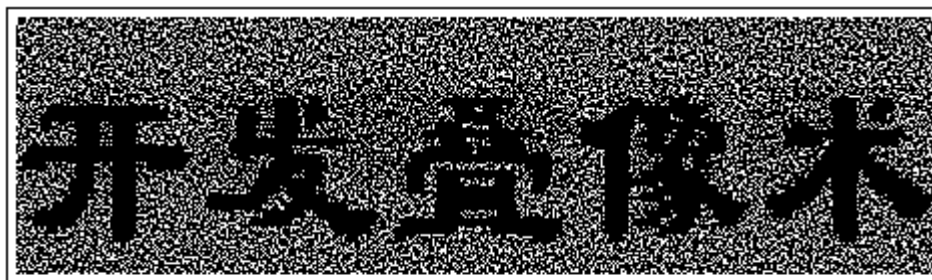
- 主要特点：恢复秘密图像时不需要任何复杂的计算，直接以人的视觉系统就可以将秘密图像辨识出来



p1 “北京邮电大学”



p2 “信息安全中心”



$p3=p1+p2$ “开发叠像术”

图2 改进后的叠像术

信息隐藏研究分支——图像取证

○ 图像取证背景

- 数码相机的快速普及，图像处理和编辑软件的广泛使用，使得修改、编辑数码照片变得越来越简单和有趣，任何人都可以轻易地完成图像的造假。



信息隐藏研究分支——图像取证



信息隐藏研究分支——图像取证

○ 图像取证

- 运用包含数字信号处理、数字水印在内的各项技术，鉴定图像的来源（数码相机、扫描仪、计算机生成、图像采集卡...），以及图像完整性（是否经过编辑？经过何种编辑？在何处被编辑？）。

分支——感知哈希

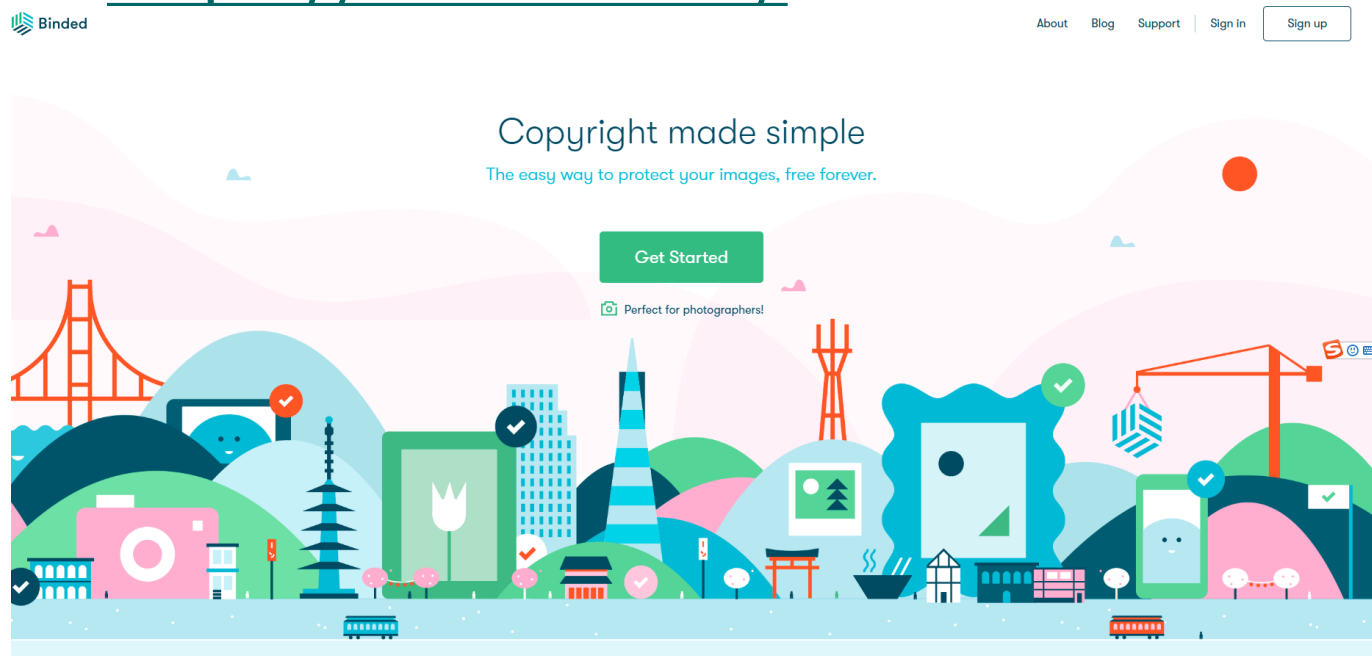
○ 感知哈希

- 图像感知哈希：由图像数据集到图像感知摘要集的一个简短的单向映射，是对图像感知信息的简短摘要
- 图像感知哈希：借鉴了密码学哈希的摘要性、单向性和抗碰撞性的同时，最重要的是要求其能够对内容保持操作具有鲁棒性，并对内容篡改操作具有敏感性
- 主要用于解决图像内容的识别和认证

数字水印技术发展趋势和应用

- 数字水印技术与区块链技术结合，保护版权

- <https://binded.com/>



总结

- 信息隐藏技术的最重要的两个分支是数字水印、隐写术。
- 数字水印主要用于版权保护。
- 隐写术主要用于保密通信。
- 数字水印嵌入载体中的信息与载体有关。
- 隐写术则嵌入与载体无关的秘密信息。
- 基于隐写术的保密通信掩盖的是通信存在的事实。

练习题

○ 判断以下说法是否正确：

1. 基于信息隐藏的保密通信，其安全性依赖于秘密信息不可懂。

○ 单选题：

1. 卡登格子是意大利数学家提出的一种信息隐藏技术，请问，它属于以下哪一类古典信息隐藏技术（）

○ A. 技术型 B. 语言学型 C. 版权保护型 D. 艺术作品型

练习题

○ 单选题：

1. 现代信息隐藏技术在哪个时期得到快速发展（）
 - A. 480 B.C. B. 19世纪70年代 C. 20世纪90年代 D. 18世纪60年代
2. 信息隐藏的研究分支不包括：（）
 - A. 隐写术 B. 数字水印 C. 隐蔽信道 D. 信息分存 E. 图像取证 F. 感知哈希 G. 流密码
3. 数字水印的应用不包括：（）
 - A. 版权保护 B. 广播监控 C. 盗版追踪 D. 内容认证 E. 拷贝控制 F. 设备控制 G. 标注 H. 保密通信

练习题

○ 思考题：

1. 分析以下应用原理，属于哪一种水印？
 - a) 使用水印相机生成一张北邮校园照片。
 - b) 制作一个包含学号信息的二维码。
 - c) 将a、b两项内容（图片）存入word文档，以班级、姓名为水印，添加到文档中。
 - d) 结合数字水印的应用，说明三种应用的功能。
2. 通过网络了解数字版权管理当前使用的现状。



概论

附录

参考资料

- MP3Stego
 - <http://www.petitcolas.net/fabien/steganography/mp3stego/>
- Benchmark(stirmark)
 - <http://www.petitcolas.net/fabien/watermarking/stirmark/index.html>
- Outguess
 - <http://www.outguess.org/>

参考资料

- Jstego
 - <http://sourceforge.net/projects/jstego/>
- Digimarc
 - <https://www.digimarc.com/about/>
- Alpha tech
 - <http://www.alphatecltd.com/>
- Bluespike
 - <http://www.bluespike.com>

参考资料

○ Data-Hiding Codes

- PROCEEDINGS OF THE IEEE, VOL. 93, NO. 12, DECEMBER 2005
- PIERRE MOULIN, FELLOW, IEEE, AND RALF KOETTER, MEMBER, IEEE

练习题解答

○ 判断以下说法是否正确：

1. 基于信息隐藏的保密通信，其安全性依赖于秘密信息不可懂。

解：**错**。信息隐藏技术是用载体作“伪装”，掩盖秘密信息的存在。因此，基于信息隐藏的保密通信，其安全性依赖于秘密信息**不可见**。

练习题解答

○ 单选题：

1. 卡登格子是意大利数学家提出的一种信息隐藏技术，请问，它属于以下哪一类古典信息隐藏技术（）
 - A. 技术型 B. 语言学型 C. 版权保护型 D. 艺术作品型
- 解：卡登格子是一种语言学型信息隐藏技术，应选B。

练习题解答

○ 单选题：

2. 现代信息隐藏技术在哪个时期得到快速发展
()

- A. 480 B.C. B. 19世纪70年代 C. 20世纪90年代 D. 18世纪60年代

○ 解：现代信息隐藏技术在**20世纪90年代**发展迅速，应选**C**。

练习题解答

○ 单选题：

3. 信息隐藏的研究分支不包括：（）

A. 隐写术 B. 数字水印 C. 隐蔽信道 D. 信息分存
E. 图像取证 F. 感知哈希 G. 流密码

解：A-F都是信息隐藏的研究分支，流密码是一种密码体制，不属于信息隐藏的研究范畴，因此，应选G。

练习题解答

○ 单选题：

4. 数字水印的应用不包括：（ ）

A. 版权保护 B. 广播监控 C. 盗版追踪 D. 内容认证
E. 拷贝控制 F. 设备控制 G. 标注 H. 保密通信

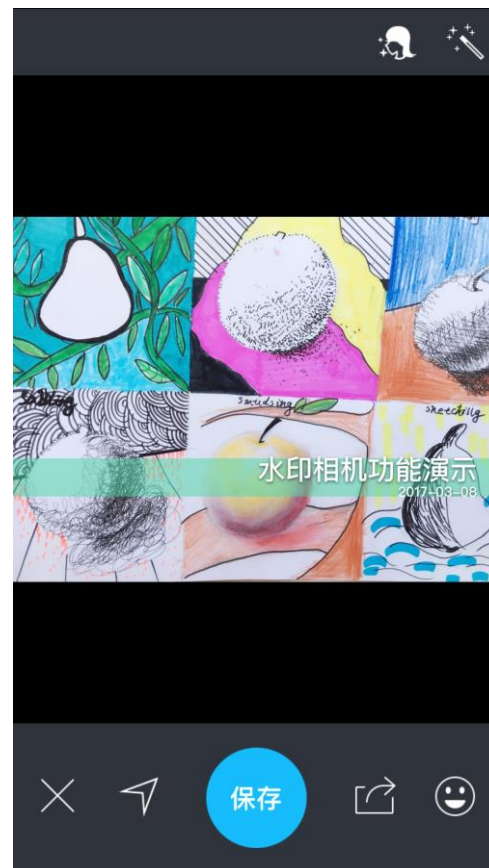
解：数字水印和隐写术是信息隐藏的两个主要研究分支。数字水印的应用包括A-G，保密通信是隐写术的主要应用。因此，应选H。

练习题解答

○ 思考题：

4. a)

解：水印相机在照片中添加文字信息，这些信息是可见的，并且与图像融为一体，是一种可见水印。水印相机是“标注”功能的特例，其添加的标注信息不是为了方便检索，而是为了丰富照片内容。



练习题解答

○ 思考题：

4. 分析以下应用原理，属于哪一种水印？

b) 制作一个包含学号信息的二维码。

解：二维码技术将信息编码为二维、二值图像，信息可以是URL、文本、标识等。应用决定了二维码的用途，例如，可用于网页导航，支付等。

二维码是一个独立、可分割的图形区域，因此，二维码并不是一种水印技术。

练习题解答

○ 思考题：

4. 分析以下应用原理，属于哪一种水印？

c)

解：word文档水印可见，与文字区域融合，是一种可见水印。

word文档水印通常包含版权声明，用于版权保护。

作为高档酒店的标识，水印也出现在了这类酒店的信纸中。添加水印并不是为了保护版权，而是为了宣传和展示。