

Computational and visual secret, trend and applications in security

DOP Shih-Jeng WANG /王旭正

- 中央警察大學 資訊管理系
- 中華民國資訊安全學會 (www.ccisa.org.tw, 理事 (2000-2012))
- 中華民國資訊安全學會 副理事長 (www.ccisa.org.tw, 2012-)
- Visiting Scholars at FSU and UF in USA, 2002, 2004, 2010.
- Academic tour for International Project Inspection at CMU in USA, 2007
- Columnists of Domestic Information-tech Magazines, <http://www.netadmin.com.tw/>
網路通訊/iThome/網管人雜誌, 2002-2006, 2007-至今
- Director of ICCL, <http://hera.im.cpu.edu.tw>
(Information Cryptology and Construction Lab.)
- sjwang@mail.cpu.edu.tw, <http://www.wretch.cc/blog/icclsjwang>

Computational and visual secret, trend and applications in security

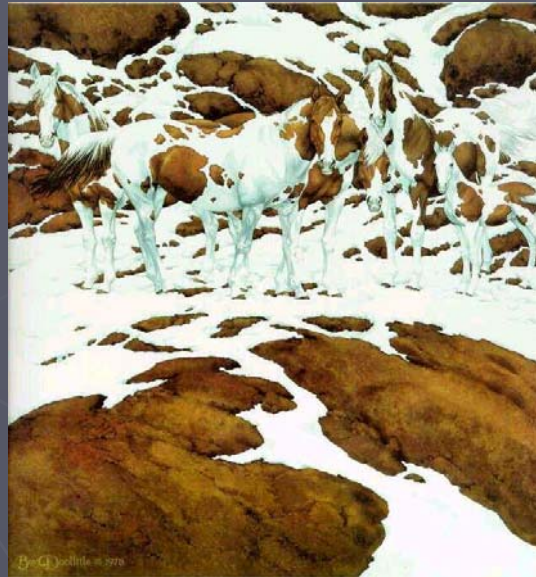
DOP Shih-Jeng **WANG** /王旭正

- 中央警察大學 資訊管理系
- 中華民國資訊安全學會 (www.ccisa.org.tw, 理事 (2000-2012))
- 中華民國資訊安全學會 副理事長 (www.ccisa.org.tw, 2012-)
- Visiting Scholars at FSU and UF in USA, 2002, 2004, 2010.
- Academic tour for International Project Inspection at CMU in USA, 2007
- Columnists of Domestic Information-tech Magazines, <http://www.netadmin.com.tw/>
網路通訊/iThome/網管人雜誌, 2002-2006, 2007-至今
- Director of ICCL, <http://hera.im.cpu.edu.tw>
(Information Cryptology and Construction Lab.)
- sjwang@mail.cpu.edu.tw, <http://www.wretch.cc/blog/icclsjwang>

視覺安全機制的時代與應用



Something you see



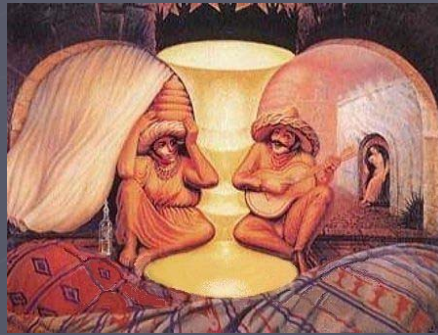
Outline

- ▶ 視覺的世界
- ▶ 黑白的世界
- ▶ 灰色的世界
- ▶ 彩色的世界
- ▶ 視覺安全的潛力
- ▶ 操之在“靈”

What is this?

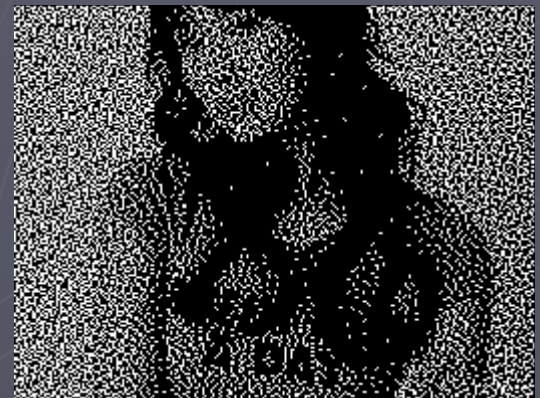
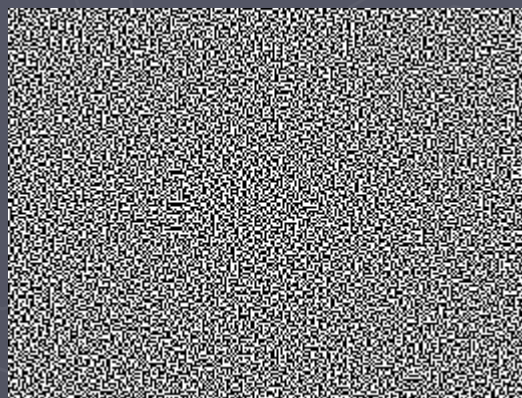
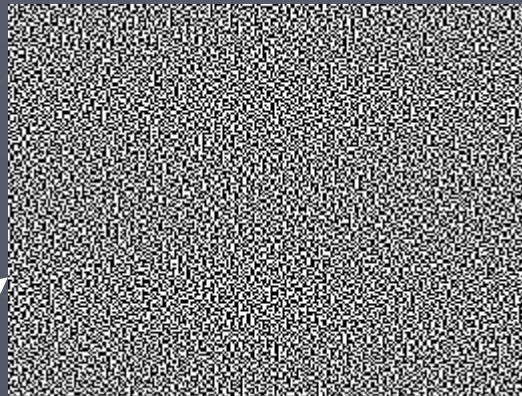
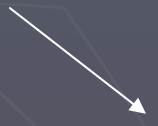
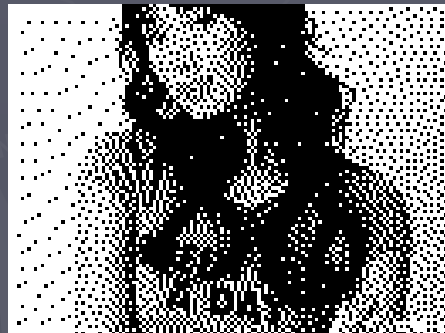
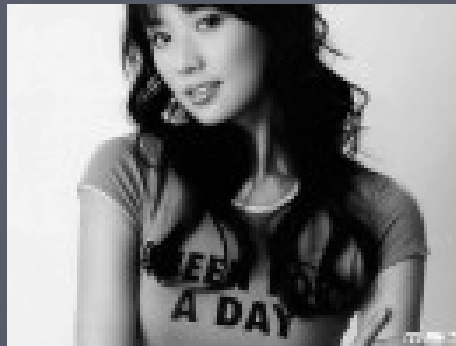


This is a couple.



Are you ready?

- ▶ Visual world, visual performance
- ▶ Security upon vision
- ▶ Cryptography, steganography
- ▶ Visual cryptography
- ▶ It is your world under your elegant applications.



視覺安全

雙方



群體

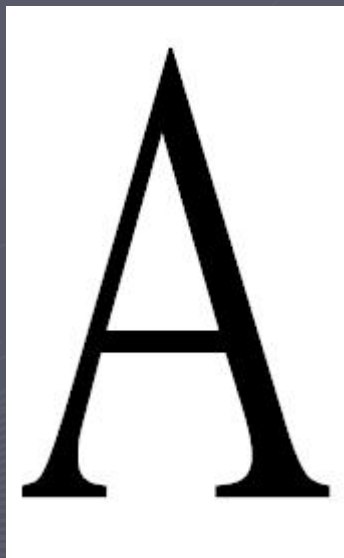
秘密分享技術

經由複雜的驗算

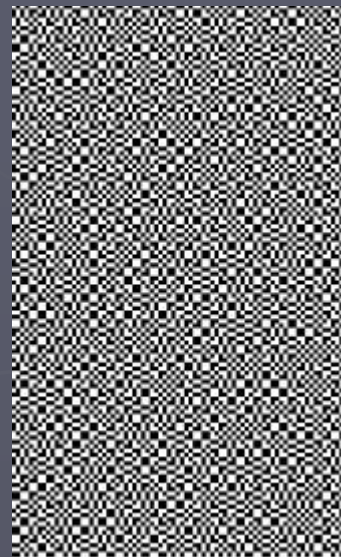
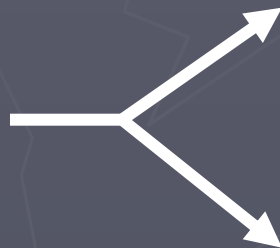


視覺系統解密

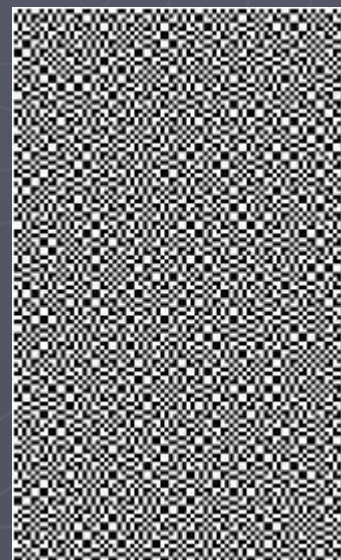
視覺安全技術



Original image

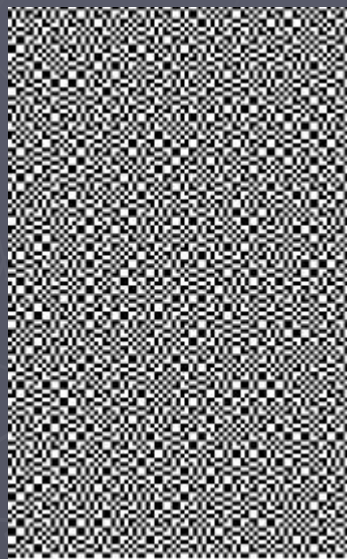


Share 1

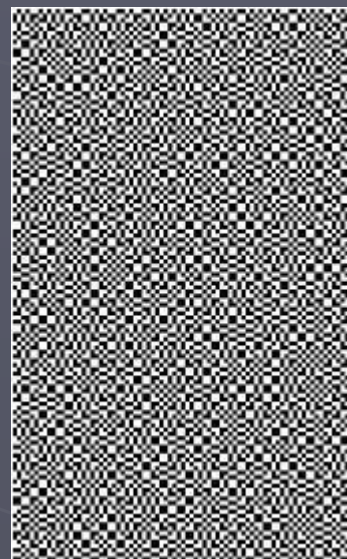


Share 2

視覺安全技術

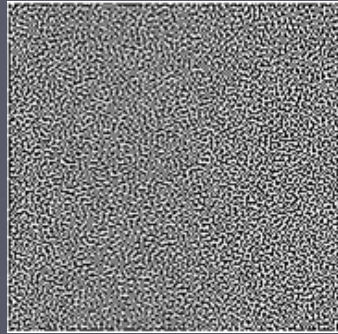


Share 1

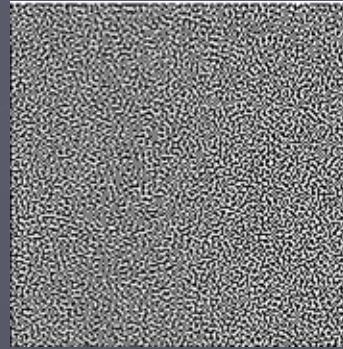


Share 2





Shadow 1

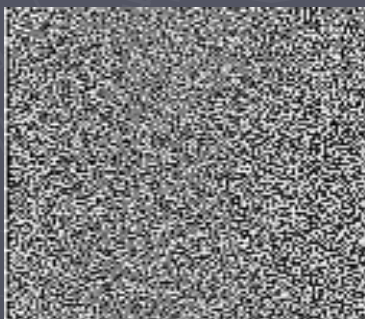
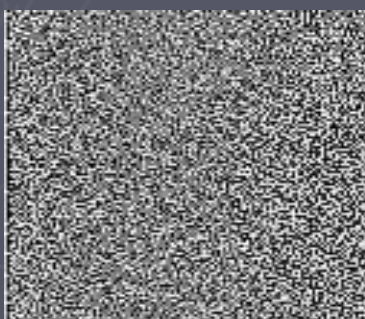
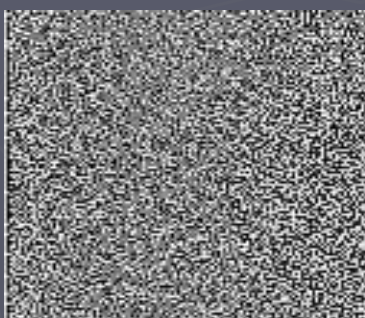
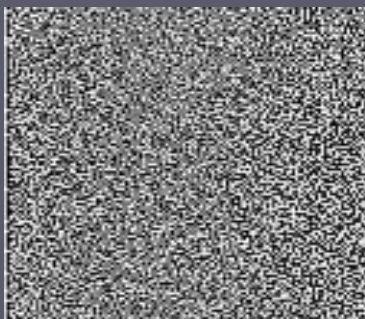


Shadow 2

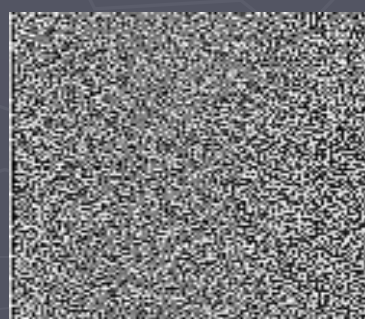
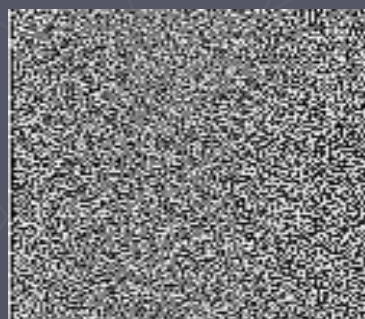
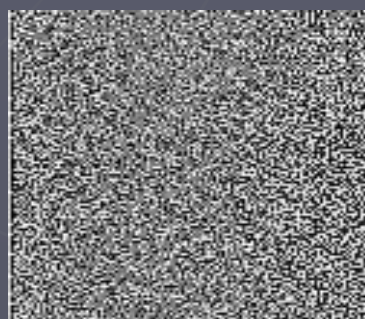
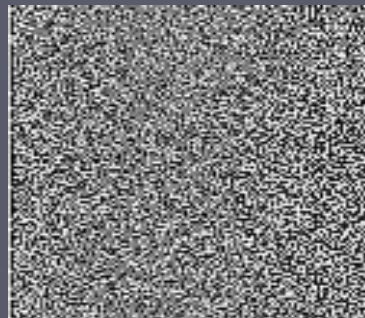


Shadow 1 + Shadow 2

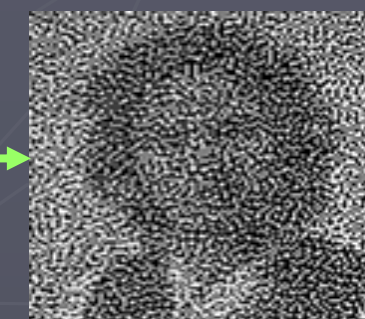
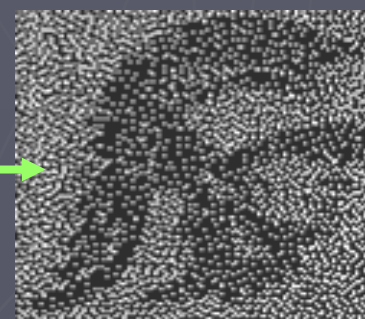
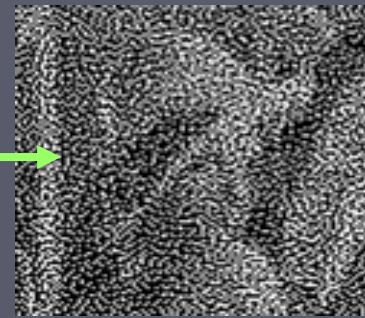
Shadow 1



Shadow 2



Overlap

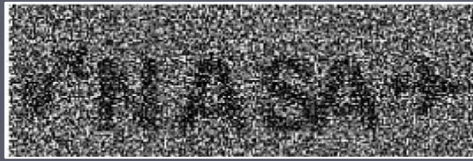


0°

90°

180°

270°



S1



S2



S3



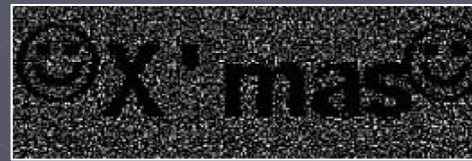
S4



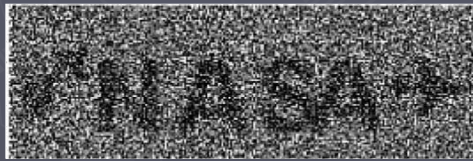
S5



+



=



+



=



+

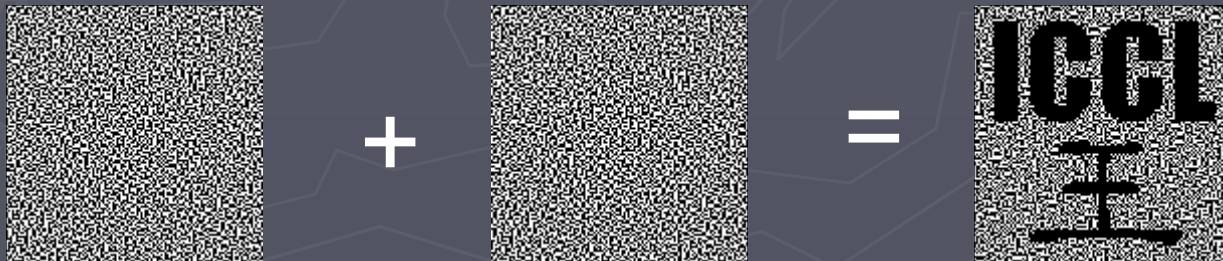


=



視覺安全(密碼)學

- ▶ 1994年Naor and Shamir 提出的方法稱為 Visual Cryptography(視覺密碼)
- ▶ 不需要像傳統的加密法要大量複雜的運算才能將秘密訊息解密。
- ▶ 不需要計算機的輔助，只需將數張圖疊合便可透過人眼解讀出其中所隱藏的機密訊息。



視覺安全

- ▶ 視覺安全能做到秘密分享機制，如
(k,n)-threshold -- 分成張分享圖，每一份在外觀上看起來都是亂碼，要有k張或k張以上疊合才能得到原訊息。
- ▶ 秘密分享機制：
將秘密資訊分給多人保管，但只有這些人將其保管的資訊結合起來，才能得到原本的訊息。

視覺安全

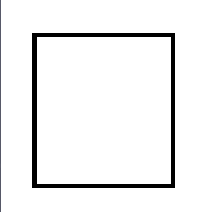


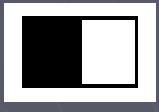



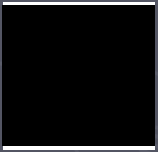


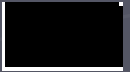


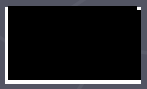
- ▶ 假如說家公司的重要金庫的鑰匙只有一把，如果說鑰匙只交給總經理保管，那我們不難想像，有一天總經理將會捲款逃跑。但如果利用上面提到的機密分享的機制來保管金庫的鑰匙，也就是說打好幾把不同的鑰匙，每把鑰匙分別發給公司的董事們，只有所有的鑰匙一起開，才能將金庫的門打開，這就是秘密分享的優點。
- ▶ 核子潛艇要發射核彈時就需要艦長與副艦長兩個人的密碼同時核准才可以發射，只有一個人的密碼是不可以發射的。

視覺安全

- ▶ 對比的性質（**Contrast**）：
在疊合的時候，秘密圖像與周圍的背影有對比上差距存在，才能得出秘密訊息。
- ▶ 安全的性質（**Security**）：
保證分享圖中無法得到任何關於圖像的訊息。

黑白視覺安全介紹

- 利用下表的定義，來決定填入的顏色:(1 x 2)

原圖像素	Share1	Share2	重疊結果
			
			
			
			

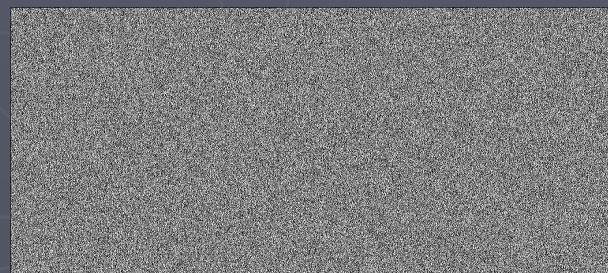
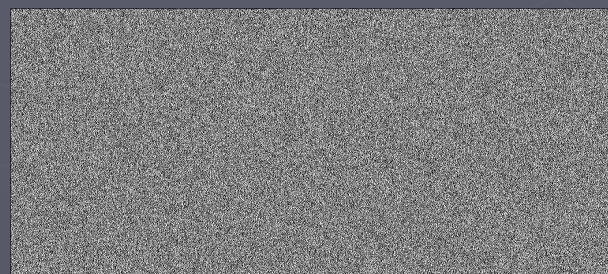
黑白視覺安全介紹

Share1

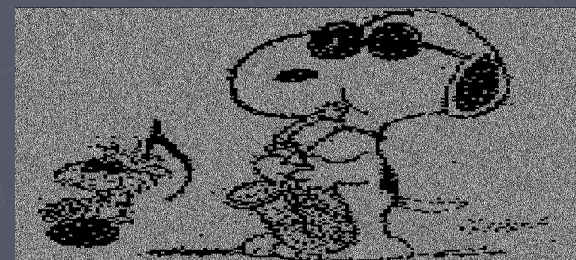


原圖

利用上表
方式分解



疊合



重疊結果

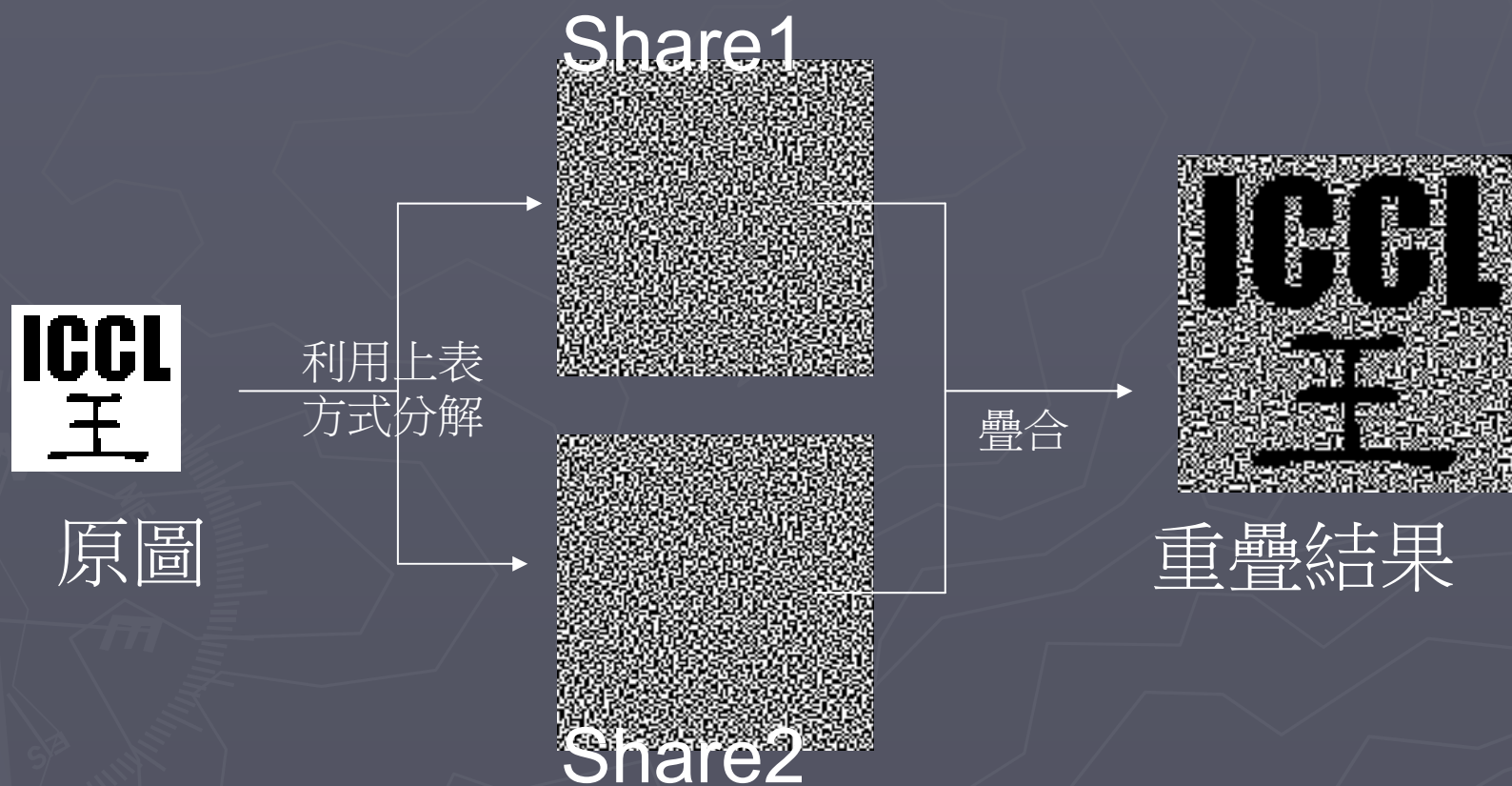
Share2

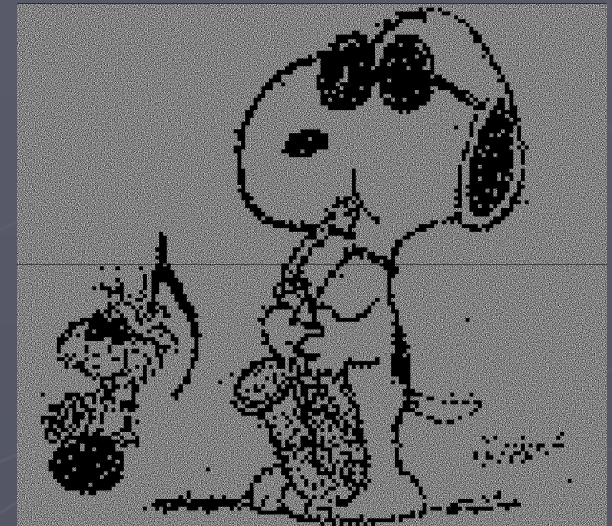
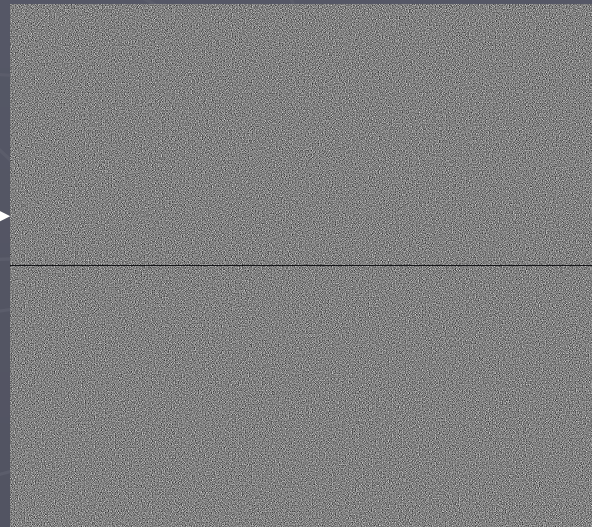
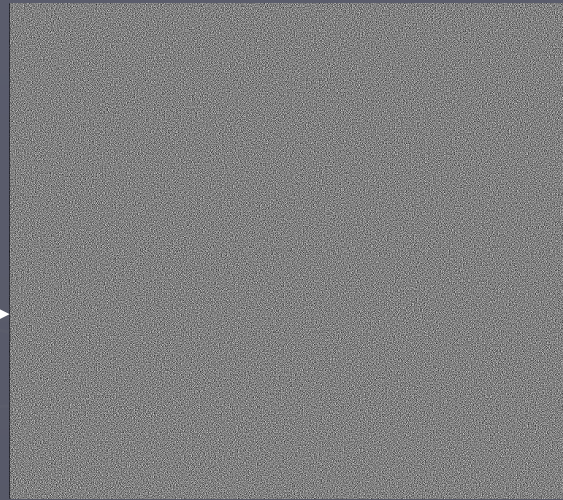
黑白視覺安全介紹 (擴張)

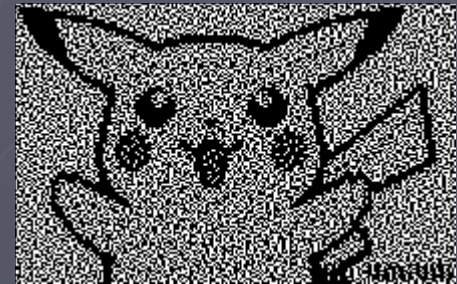
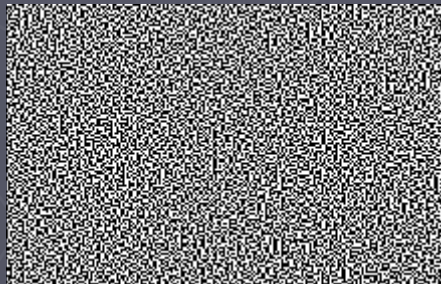
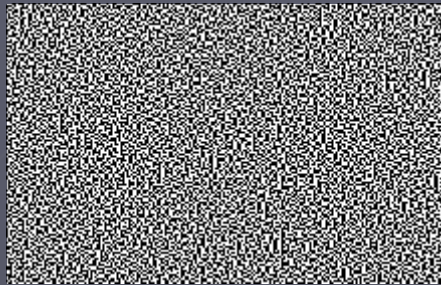
- ▶ 1X2的方法會使的影像被拉長，導致變形，應此可以始用2X2的方式來改善此缺點。

原圖像素	Share1	Share2	重疊結果
			
			
			
			

黑白視覺安全介紹(擴張)





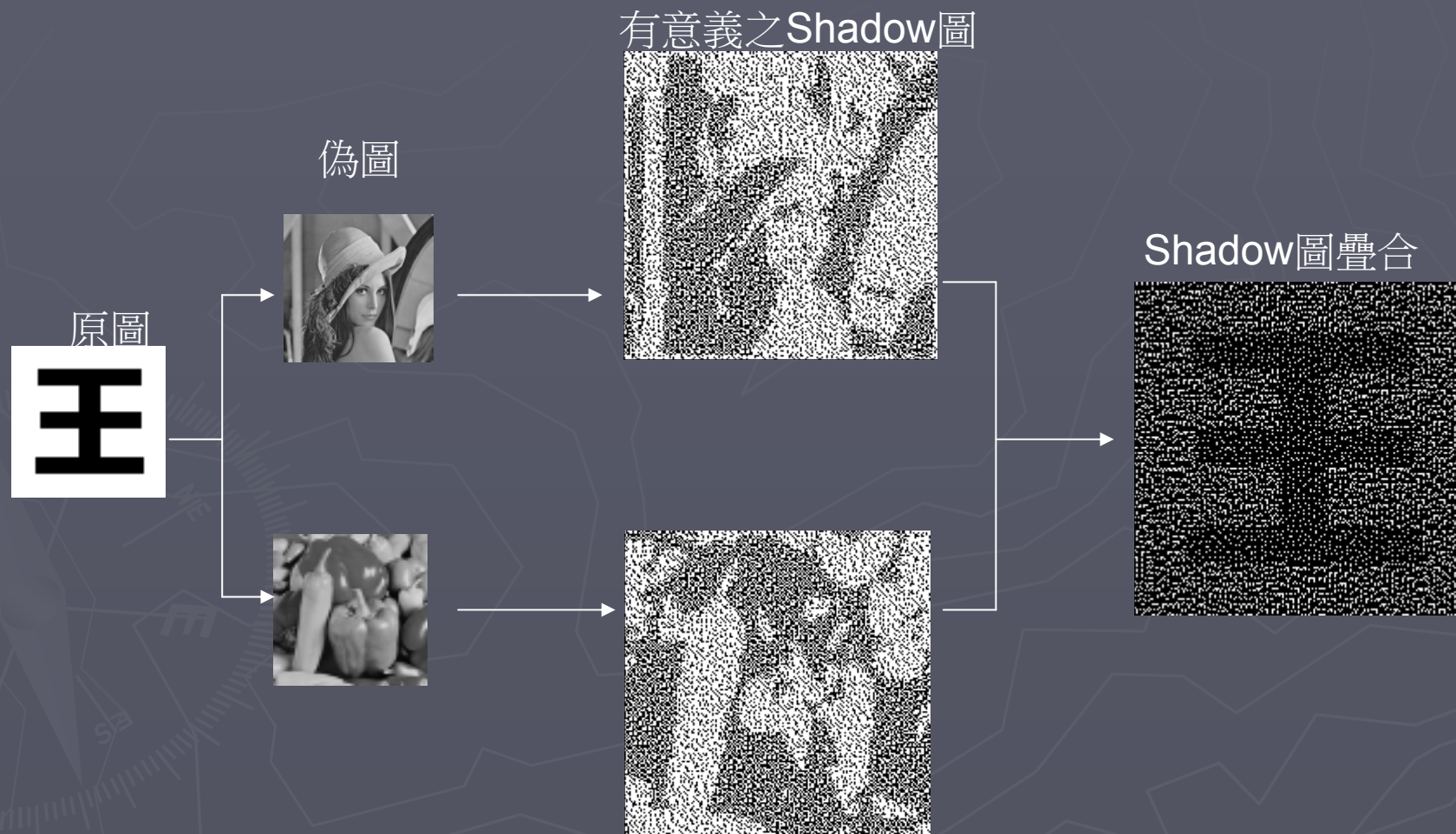


黑白視覺安全介紹(3x3)

原圖	分享圖一	分享圖二	疊合後
白			
			白
			白
			白
			白

原圖	分享圖一	分享圖二	疊合後
黑			
			黑
			黑
			黑
			黑

黑白視覺安全介紹(擴張、有意義)

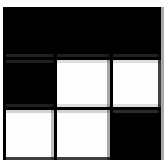
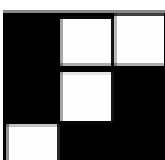
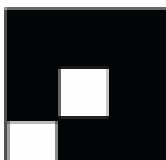
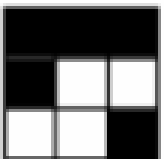
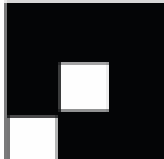
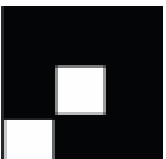
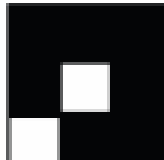
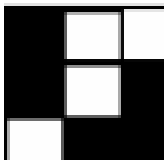
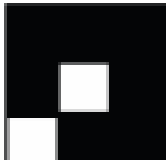
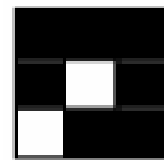
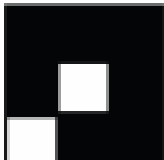
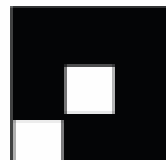


黑白視覺安全介紹(擴張、有意義)

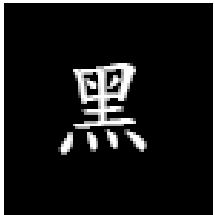
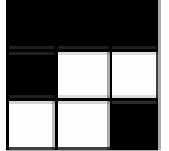
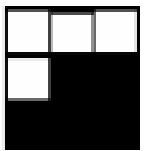
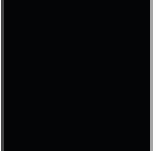
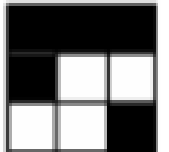
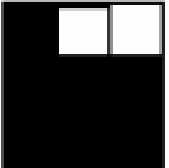

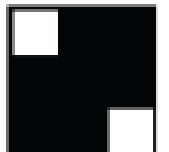
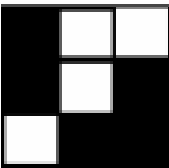

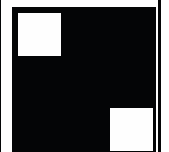
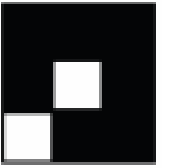
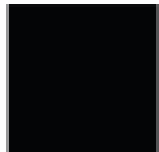
規則:

1X1	白色(偽圖)	黑色(偽圖)
Share圖 (3x3) (偽圖的擴張)	5黑4白	7黑2白
1x1	白色(原圖)	黑色(原圖)
疊合圖 (3x3)	7黑2白	9黑0白

黑白視覺安全介紹

原圖	分享圖一	分享圖二	疊合後
白			
	白(偽圖)	白(偽圖)	白
			
	白(偽圖)	黑(偽圖)	白
			
	黑(偽圖)	白(偽圖)	白
			
	黑(偽圖)	黑(偽圖)	白

黑白視覺安全介紹

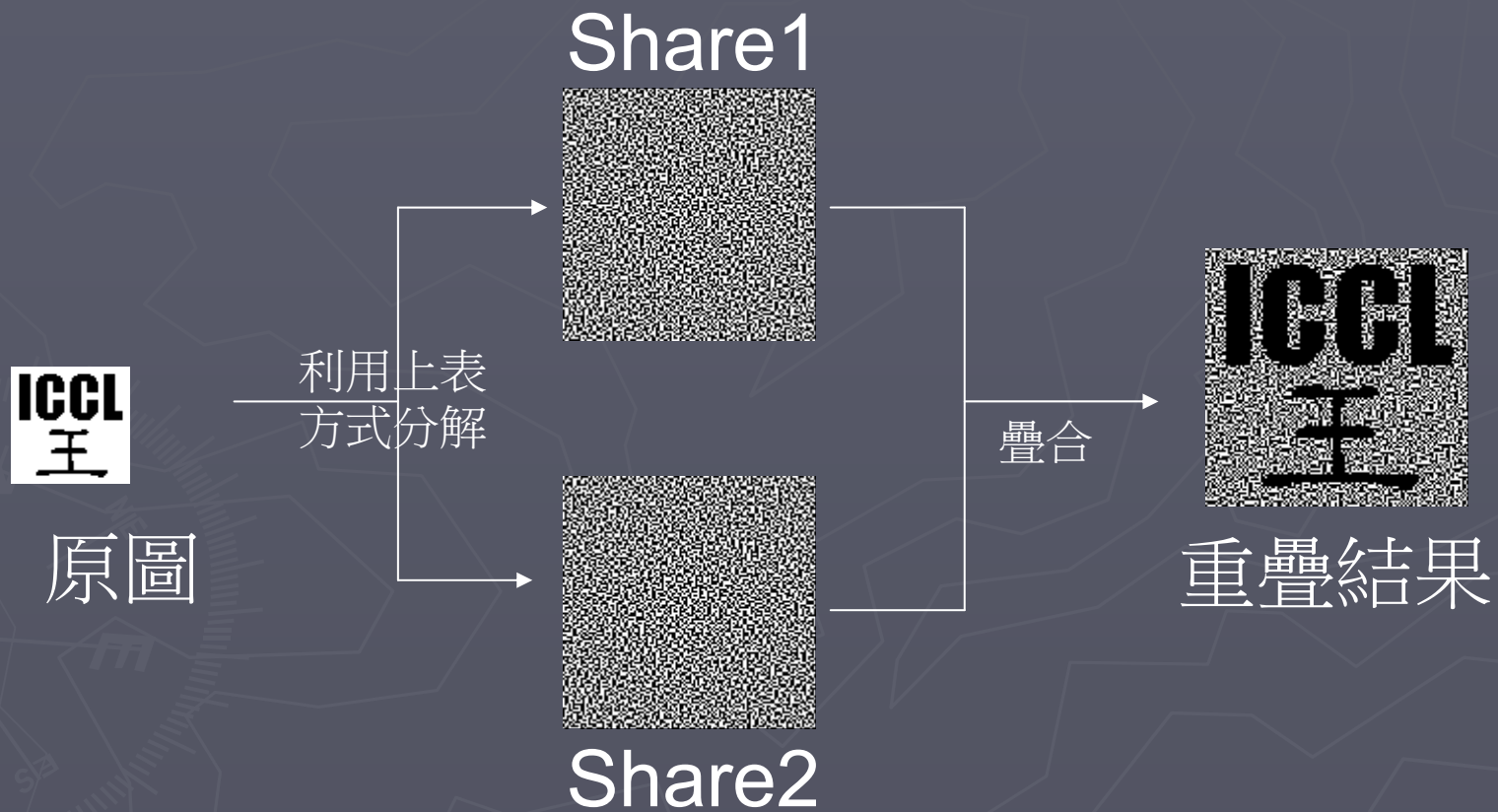
原圖	分享圖一	分享圖二	疊合後
			
	白(偽圖)	白(偽圖)	黑
			
	白(偽圖)	黑(偽圖)	黑
			
	黑(偽圖)	白(偽圖)	黑
			
	黑(偽圖)	黑(偽圖)	黑

黑白視覺安全(不擴)



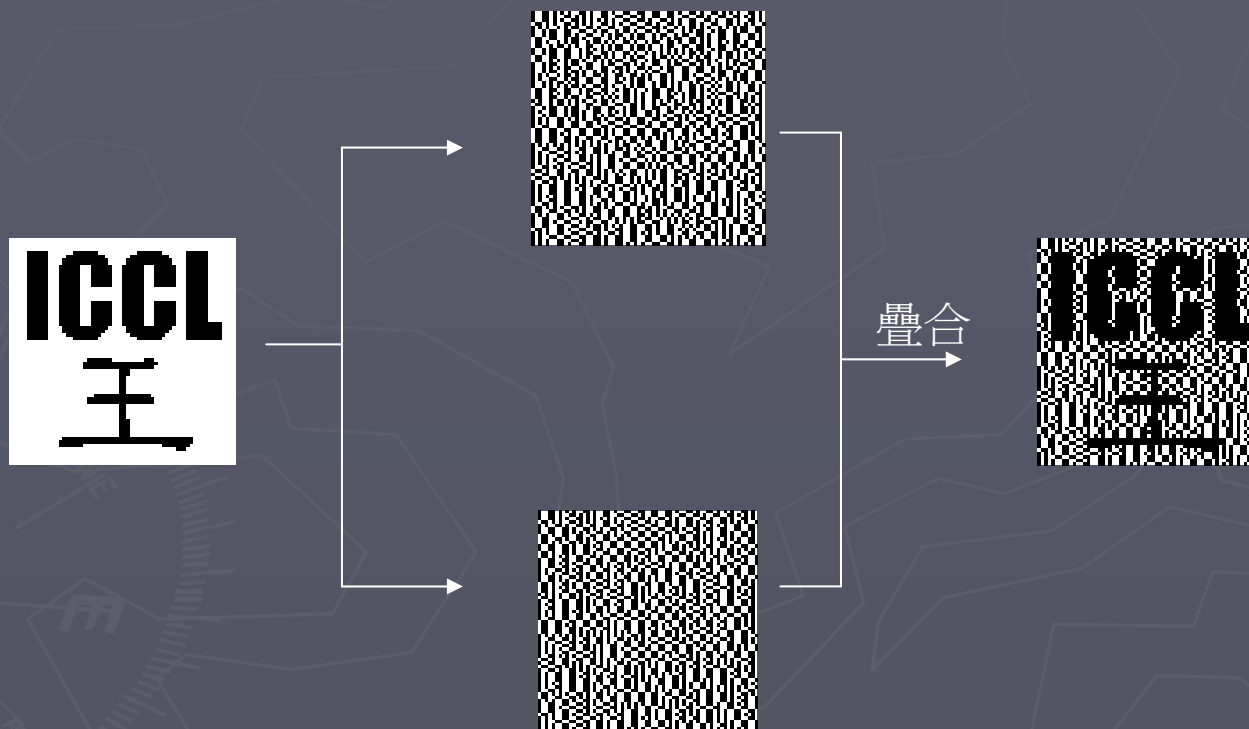
Review

黑白視覺安全介紹(擴)











































黑白視覺安全(不擴)

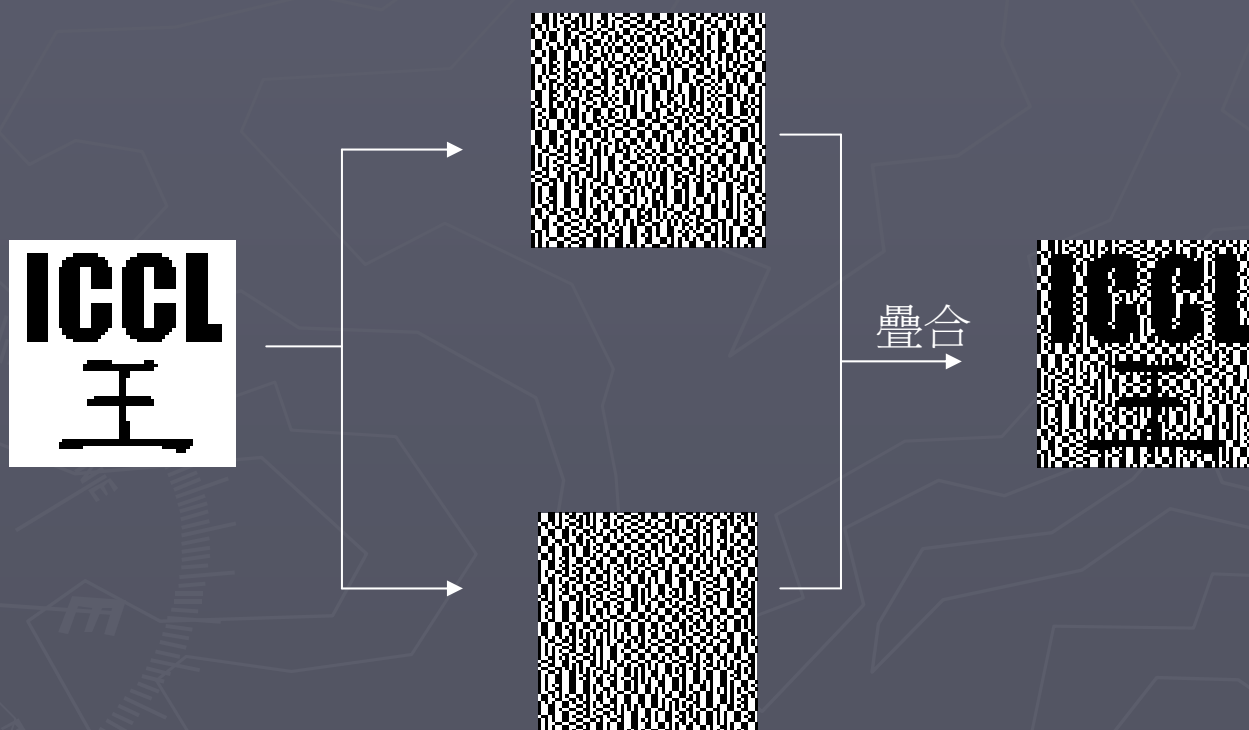
Difference ?



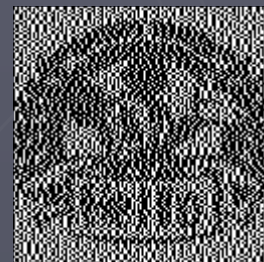
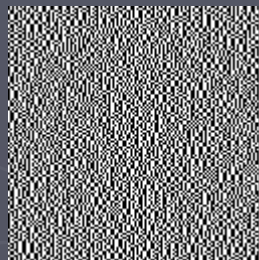
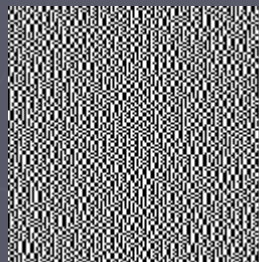
黑白視覺安全(不擴張)

加密序列	機率	加密規則		疊合結果
		分享影像 1	分享影像 2	
	0.5			
	0.5			
	0.5			
	0.5			
	0.25			
	0.25			
	0.25			
	0.25			
	0.25			
	0.25			
	0.25			
	0.25			

黑白視覺安全(不擴張)



黑白視覺安全 sample(不擴張)



灰階視覺安全

► HALFTONE :

利用網點的疏密來模擬各種不同色階的感覺



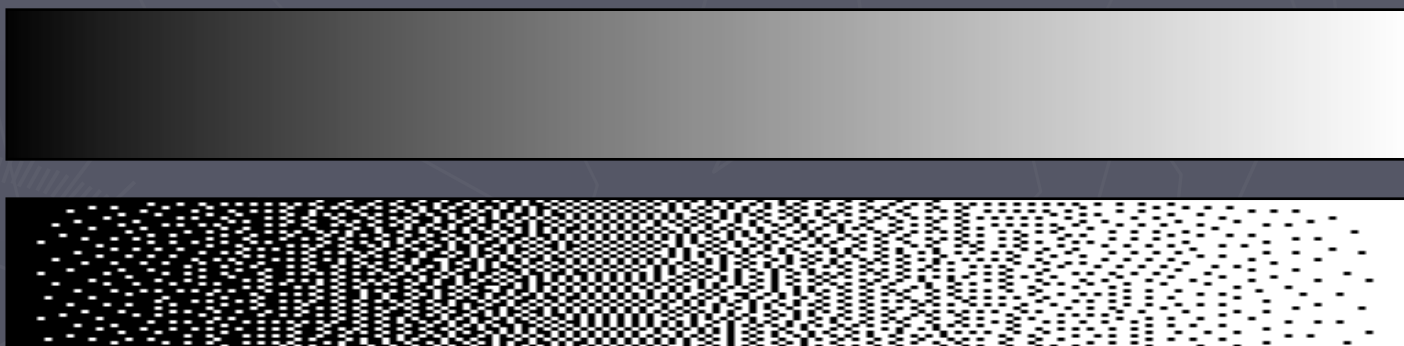
原圖



經過HALFTONE技術後

灰階視覺安全

► HALFTONE :

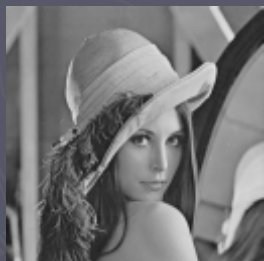


灰階視覺安全

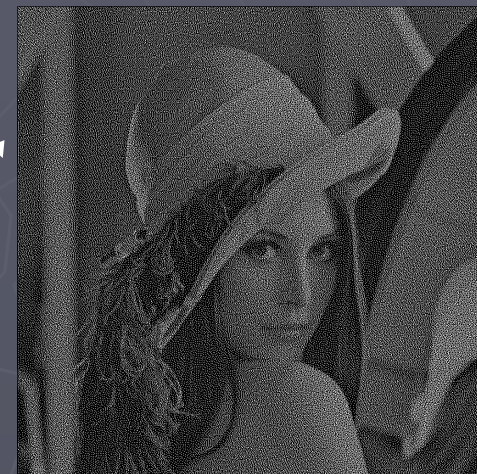
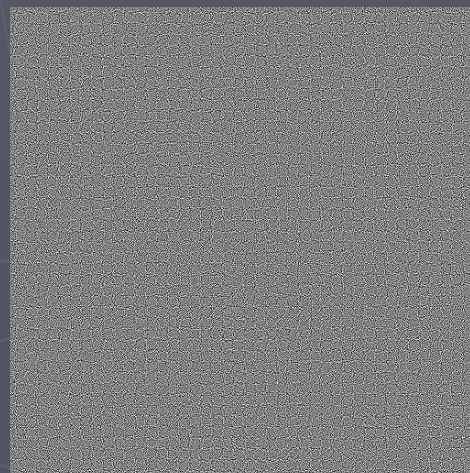
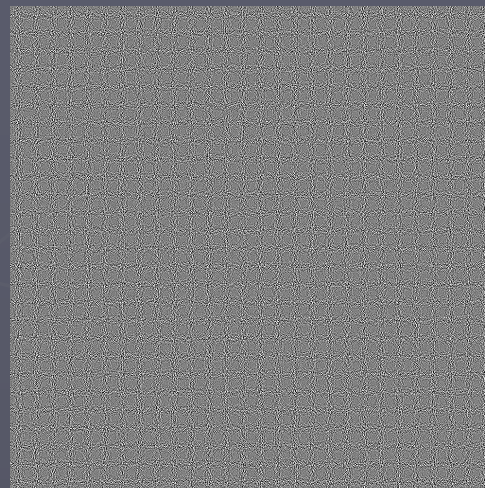
- ▶ 利用Halftone 技術將灰階影像轉為黑白
- ▶ 再利用以上黑白影像方式處理

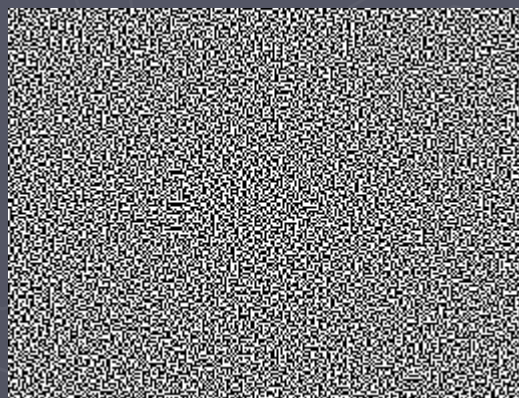
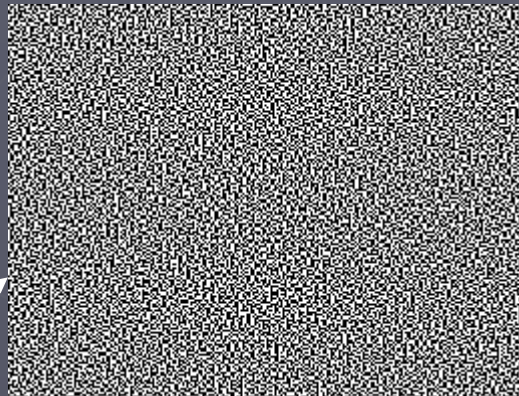
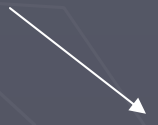
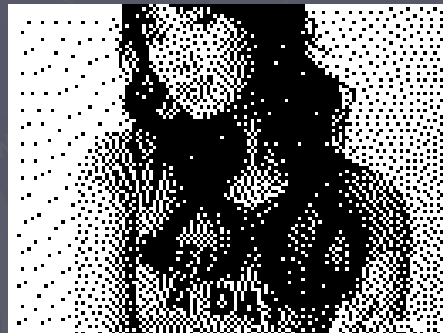
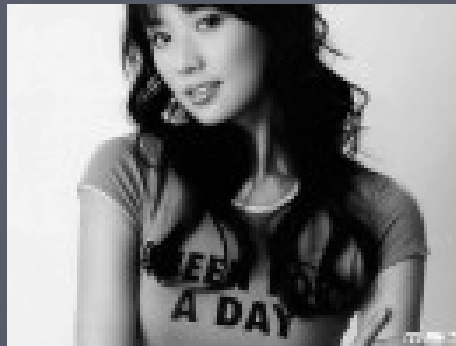
灰階視覺安全

HALFTONE技術

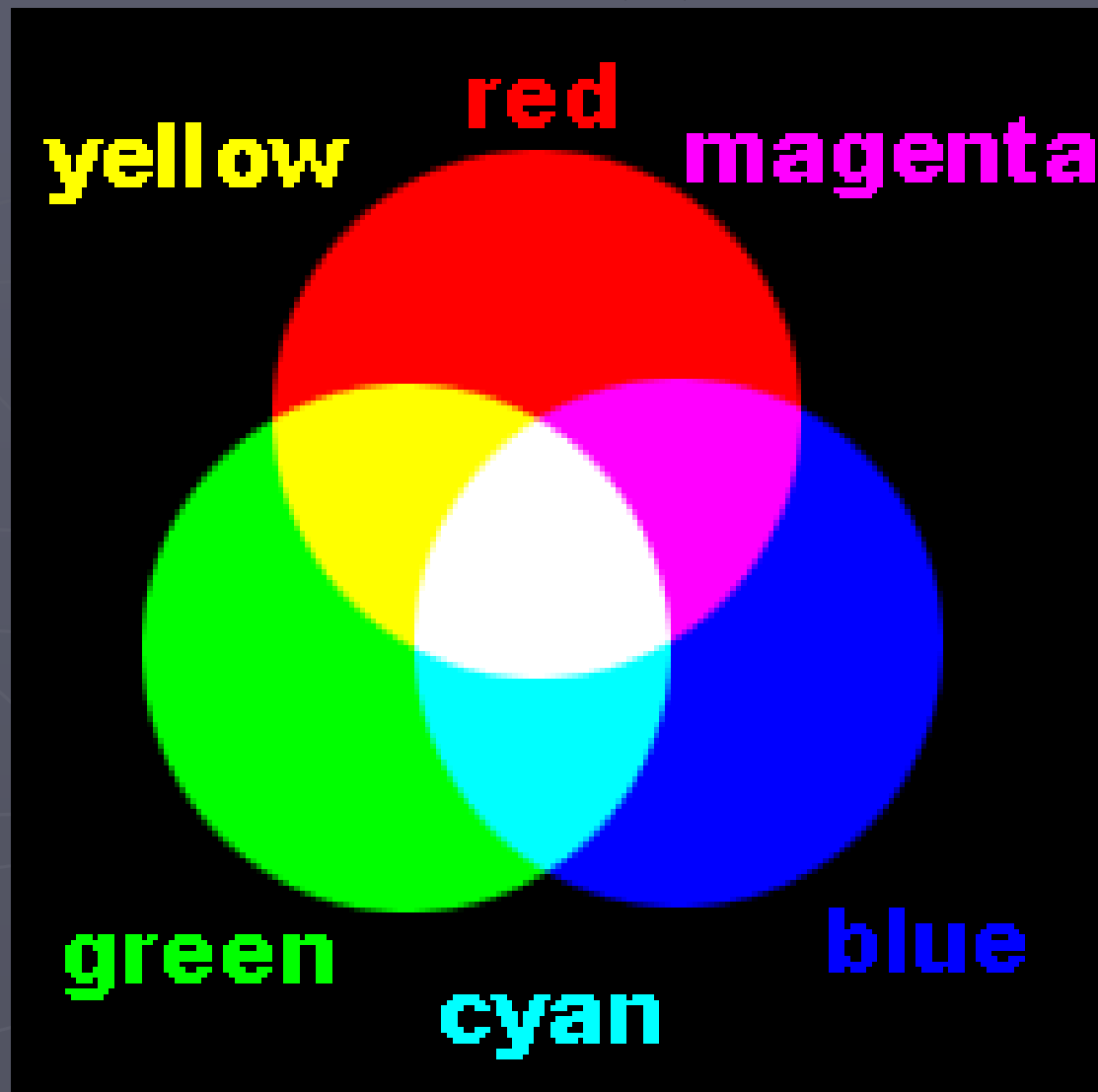


原灰階圖

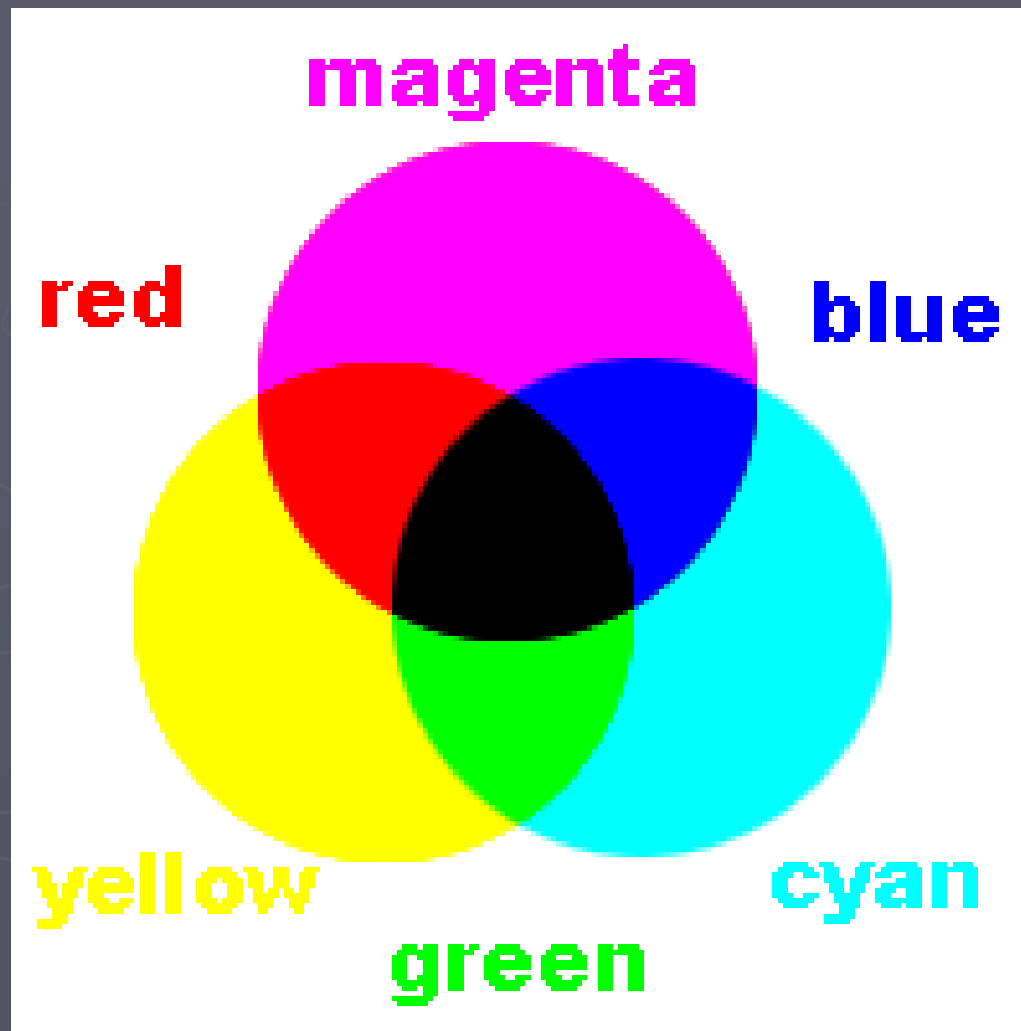


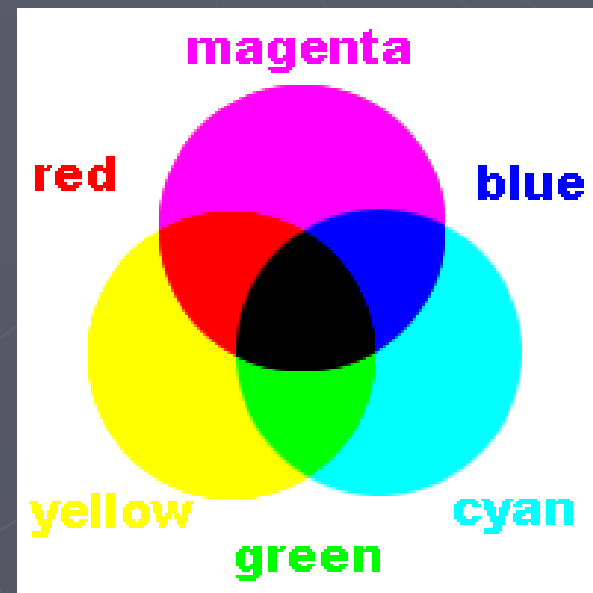
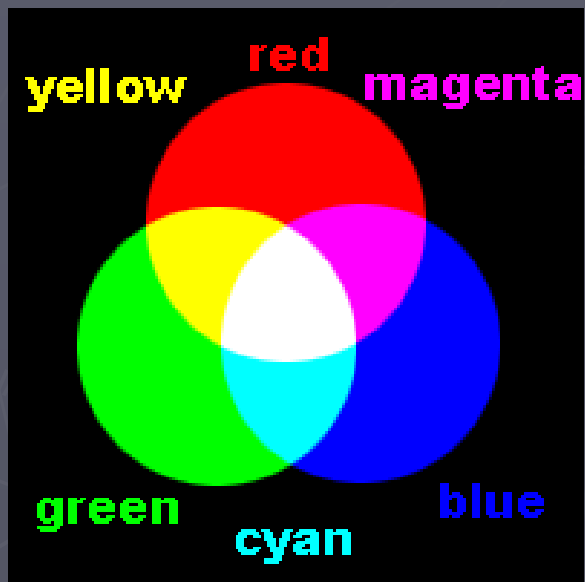


Our Life (I)



Our Life (II)

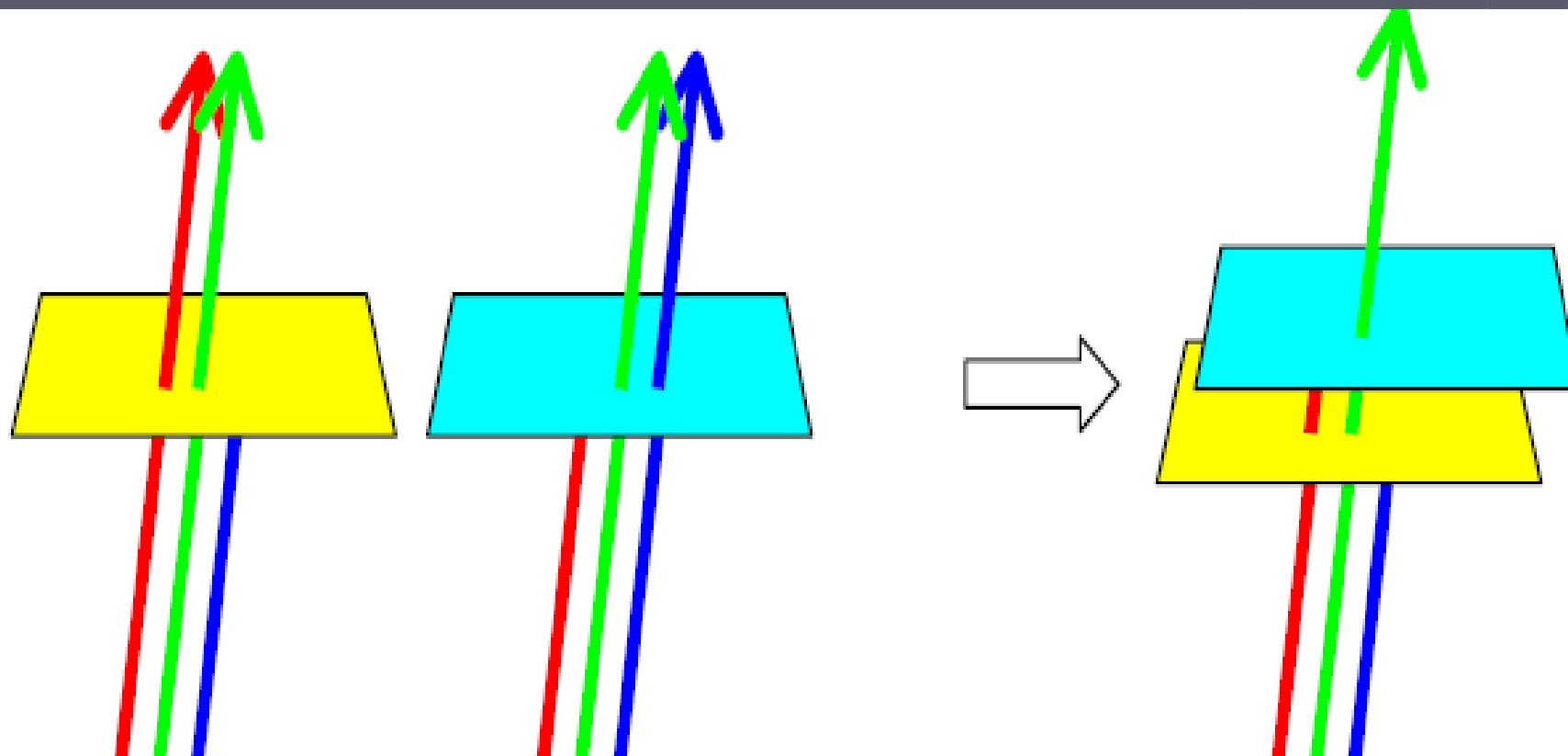




彩色視覺安全

- ▶ 一般在電腦上顯示的都是以RGB (Red, Green, Blue) Color Model來表示
- ▶ 但是視覺密碼學大部分要印在透明的投影片上來進行疊合，應此採用CMY (Cyan青, Magenta洋紅, Yellow黃) Color Model。

彩色視覺安全



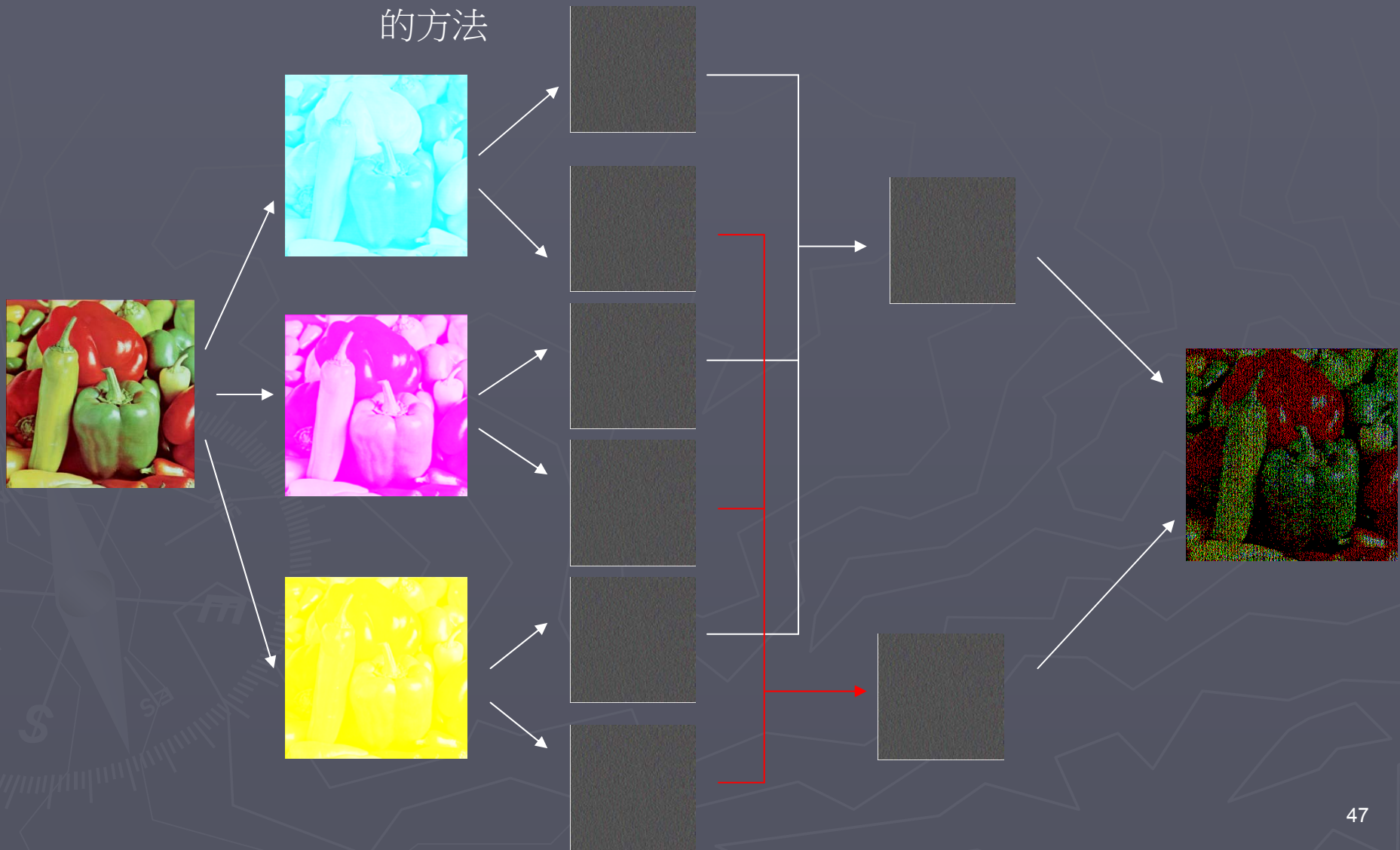
(a) 黃色的投影片

(b) 青色的投影片

(c) 疊合後得到綠色

彩色視覺安全

利用黑白視覺密碼學
的方法



彩色視覺安全(不擴張)

- ▶ 1、將彩色機密影像利用CMY模型分解成三張單一色調的影像C、M、Y。
- ▶ 2、將三張影像各轉成半色調影像C'M'Y'
- ▶ 3、再利用黑白不擴張的方法來對C'M'Y'三張影像做
處理
- ▶ 4、再將C'M'Y'處理過第 i 張分享影像合併成為一張分享影像，
- ▶ 5、最後將分享影像結合就可得到原機密影像

視覺安全(應用 I-concept)

Client

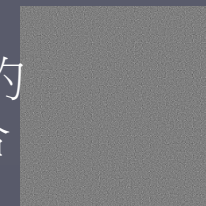
Server

由Server核發的Share圖，當作是密碼



登入時傳送

和儲存於Server端的另一個Share圖疊合

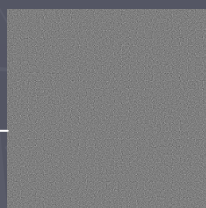


1234

使用者得到此密碼再輸入至Server端

輸入1234

登入至系統，而系統再產生另一組密碼如5678，並將配合的Share圖傳至Client端做下次登入使用



視覺安全(應用II-demo)

- ▶ 智慧財產權
- ▶ 影像竄改與偵測
- ▶ 資訊隱藏

視覺安全(應用III-feature)

- 視覺分享於身份鑑定的應用兼具簡易管理的特性。
- 解決了機密資料易被內部人員獨立盜取的問題。



視覺安全(應用III-1)



公開資料的萃取

利用CTP(二元碼至影像像素的轉換規則)表對照

使用者提供

Share- A_{i1}



產生公開資料如：

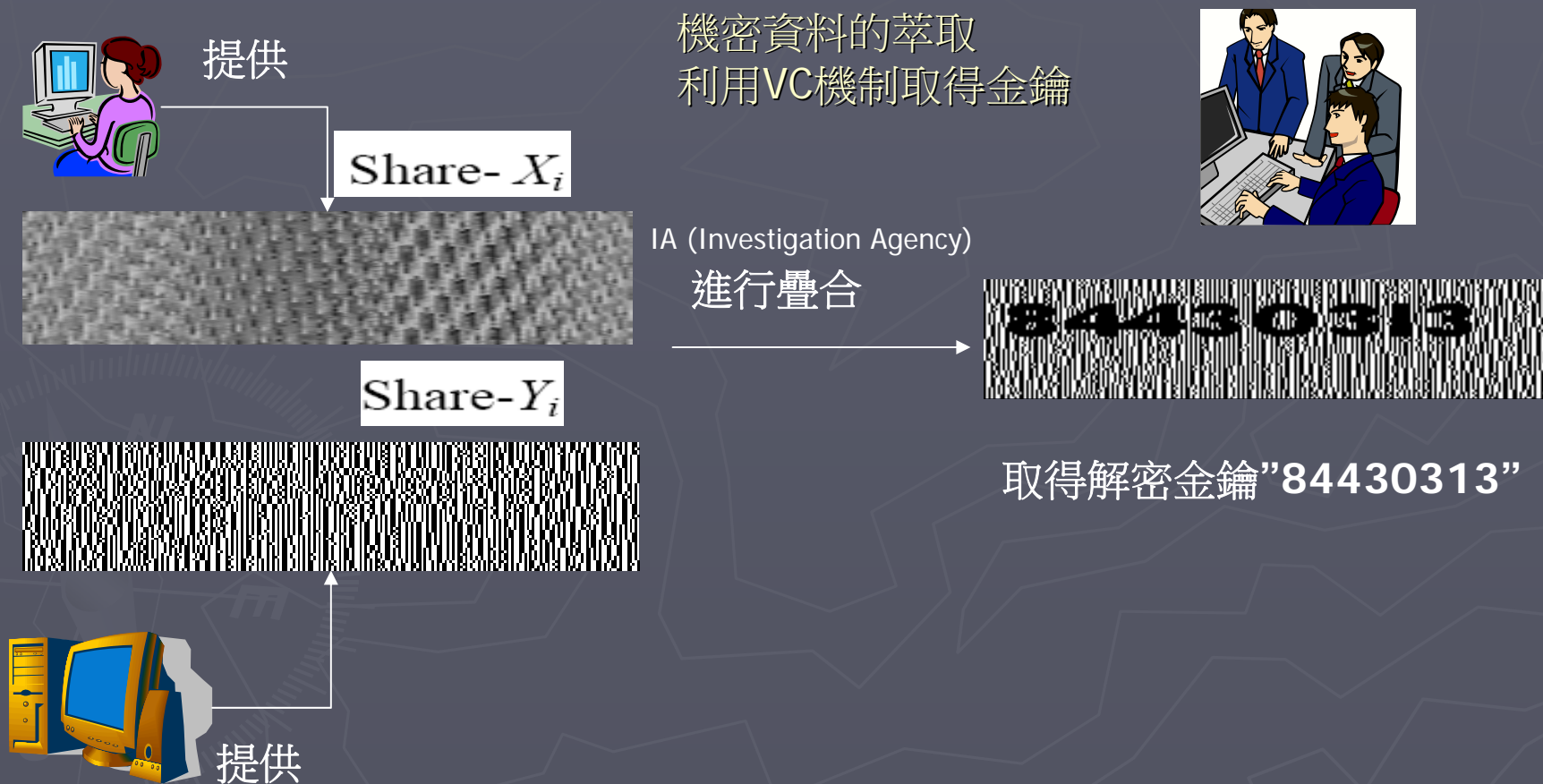
姓名、出生年月日

住址、電話等等

二元碼至影像像素的轉換規則

原始資料/擴展後	原二元碼值	轉換成像素	擴展成3倍的組合
機密資料/TI	1	B	三個B
	0	W	兩個B一個W
資本資料/Share-A	1	B	兩個B一個W
	0	W	一個B兩個W
NULL /Share-B	無	無	兩個B一個W

視覺安全(應用III-2)



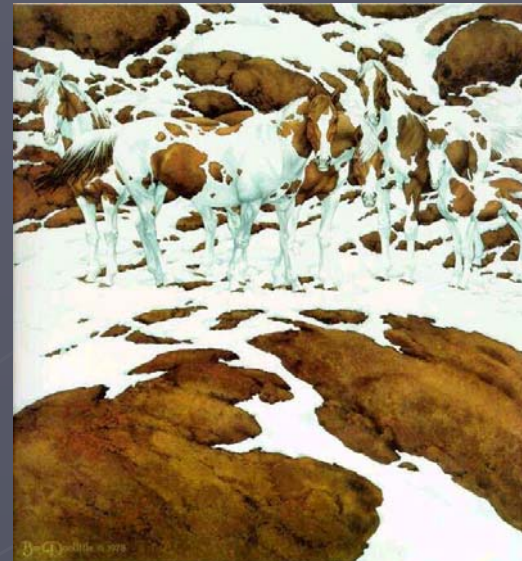
結語

Q: 網路成長快速，使各種生活應用也隨之成長。但伴隨而來的泛資訊化、資訊安全與多媒體資料在網路傳遞的安全已成為系統建置的必要議題。

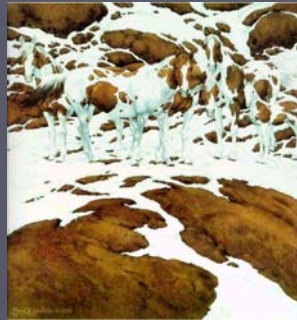
A: 倘若(IF)安全機制從基本認知開始做起，從事安全技術/管理的培養與紮根，則(THEN)安全功能(PKI導向的資安意識/機制)亦才可發揮真正效用。

Here you go

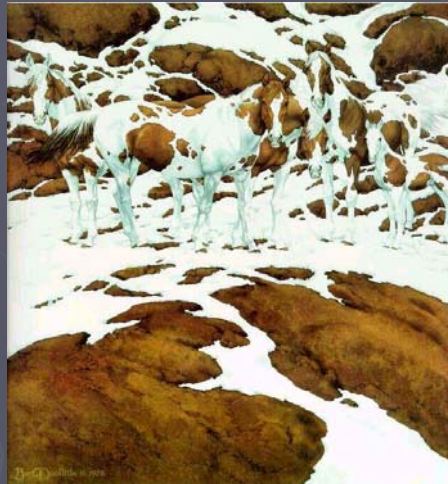
In first Jan. 2008,
AM, so amazing view in Tokyo,
can we see it again next year?
Count it to begin our expectations.



Something you see (I)

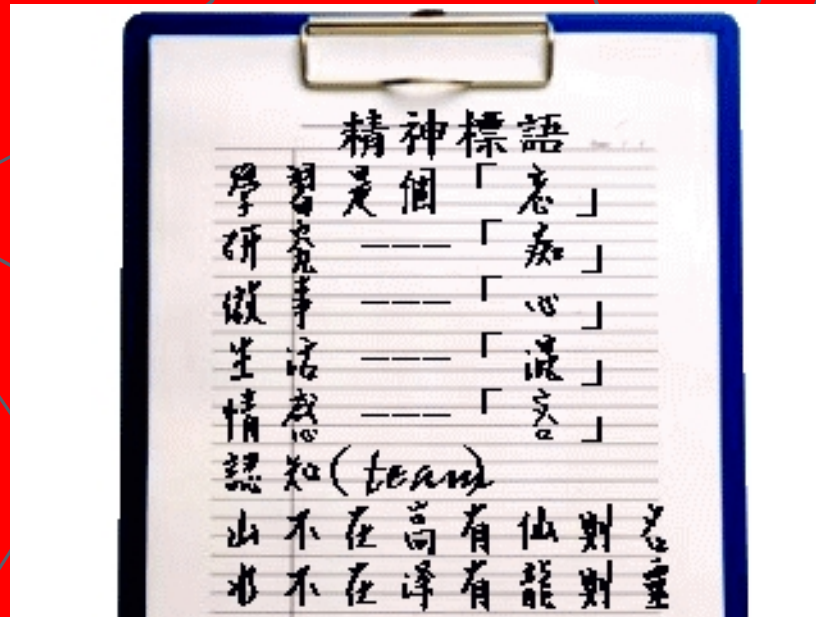
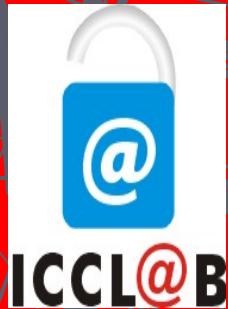


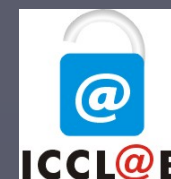
Something you see (II)



Appreciations

Everything, learning is from now on, ...





- ▶ **Dr. Professor Shiuh-Jeng WANG**
- ▶ PhD. National Taiwan University, Taiwan, 1996
- ▶ Full Professor, Central Police University, Dept. of Information Management
- ▶ Director Information Crypto and Construction Lab
- ▶ Chair of ICCL-FROG (Forensic Research development task force Group)
- ▶ Vice-President, Chinese Cryptography Information Security Association (www.ccisa.org.tw)

- ▶ Chairs of IEEE-CS/LNCS Proceedings, Internat'l confs.
<http://www.sersc.org/SH08/> <http://www.ftg.org/MPIS2009>
<http://ncs2009.ntpu.edu.tw/CI/CI.htm> <http://www.ftg.org/futuretech2010>
<https://sites.google.com/site/uicuiipm2012/> IEEE-sponsored,
<http://www.ftraf.org/music2012>
- ▶ Editor-in-Chief AT JITAS (<http://jitas.im.cpu.edu.tw>)
- ▶ SCI-Journals, Guest-editors-,
 - IEEE J-SAC, <http://www.comsoc.org/livepubs/sac/index.html>
http://hera.im.cpu.edu.tw/sjw_2006/meeting_report/IEEE-GUEST-EDITORIAL-0808-2011-.pdf
 - Journal of Internet Technology (JIT)
<http://jit.ndhu.edu.tw/callforpaper/April-2011-SI-JIT.pdf>
 - The Computer Journal, <http://comjnl.oxfordjournals.org/>
 - Springer Telecommunication Systems
<http://www.springer.com/business/business+information+systems/journal/11235>
 - The Journal of Supercomputing,
<http://www.springer.com/computer/swe/journal/11227> (Springer)
 - Peer-to-Peer Networking and Applications,
<http://www.editorialmanager.com/ppna/> (Springer)

INFORMATION
CRYPTOLOGY &
CONSTRUCTION LAB
(ICCL)