图像的复数表示及其在图像秘密分存中的应用

孙 伟[1] 杨志华[1] 齐东旭[1,2]

[1](中山大学信息科学与技术学院,广州 510275) [2](澳门科技大学资讯学院,澳门)

摘 要 针对传统图像处理中图像的表示和运算问题,提出了在复平面上表示图像的新思想,并给出了图像和复平面上点的映射算法,即换一个角度用复数运算定义了图像和图像间的"加"、"减"、"乘"、"共轭"等运算关系;同时,将其与经典的数值分存方案相结合,用于数字图像的秘密分存。实验结果表明,该方法有效解决了图像信息秘密分存中的色彩效果和像素膨胀等问题。

关键词 数字图像 秘密分存 数系 复数基

中图法分类号: TP309.7 TP391.41 **文献标识码**: A **文章编号**: 1006-8961(2004)11-1331-05

The Conversion Method From Image to Complex Number and Its Application in Image Secret Sharing

SUN Wei[1], YANG Zhi-hua[1], QI Dong-xu[1,2]

[1](*School of Information Science and Technology, Zhongshan University, Guangzhou* 510275)

[2](*Faculty of Information Technology, Macao University of Science and Technology, Macao*)

Abstract Concerning the image expression and operation problem of traditional image processing, the novel idea that expressing an image in complex plane is proposed. The conversion method of mapping image to complex number is presented, and the operations of addition, subtraction, multiplication and complex conjugate of image are defined in a new point of veiw. Hence, Combined with the existing threshold access structures scheme, it leads to proposal of using complex number based secret sharing schemes in color images sharing. Experimental results validated that it effectively solved the problems of the size of the shares and the number of colors, etc.

Keywords digital image, secret sharing, number system, complex number basis

1 引 言

(t,n)-门限密钥分散管理的概念是 Shamir 在 1979 年提出的[1]。同时,Blakley 由几何做图问题也构造了类似的方案[2]。(t,n)-门限方案是将一个密钥分解为 n 部分(子密钥),并分别交给 n 个人保管,该分解算法对于确定的整数 $t(0<t\leqslant n)$,需满足如下两个条件:(1)原始密钥可以由任意不少于 t 个人的合作获得;(2)任意少于 t 个人都无法获得原始密钥的任何信息。这里 t 通常称为方案的门限或阈值。在此后的研究中,又陆续出现了基于素数的 Asmuth-bloom 方案和基于矩阵乘法的 Karnin-Grene-Hellman 方案等等[3]。在 1994 年的 EUROCRYPT '94 会议上,Shamir 又提出了一种基于密钥分存的视觉密码学方法[4]。在随后的几年中,视觉密码学发展很快,许多有关这一问题的文章陆续发表。例如 Yue 和 Chiang 提出了基于神经网络的黑白图像分存方案[5],Chang 通过重新定义颜色索引表的方法提出了彩色图像的可视分存方案[6],并且在其后的研究中又提出更为有效的分存方案,将一幅灰度图像隐藏于不同影子图像之中,并大大提高了图像分存中的像素膨胀问题[7]。

图像的代数运算作为图像处理的基本理论,有着广泛的应用[8]。代数运算是指对两幅输入图像进行点对点的加、减、乘或除计算而得到输出图像的运

基金项目:国家"973"项目(G1998030608);国家自然科学基金项目(60133020,10071087)

收稿日期:2004-06-18;**改回日期**:2004-08-27

算。对于相加和相乘的情形，可能不止有两幅图像参加运算。在一般情况下，输入图像之一可能为常数，然而，加、减、乘、除一个常数可按线性的点运算来对待；当两幅输入图像完全相同时，也如此。另外，还可通过适当的组合来形成涉及几幅图像的复合代数运算方程。

由于在现代计算机系统中是用二进制表示图像编码的，因此，图像的代数运算也基于二进制或十进制系统。众所周知，每一个代数都存在着基底，利用它，代数中的所有元素都能唯一地表示为系数属于基本域的线性组合的形式。实际上，任意非负整数 p，都可用以下以大于 1 的正整数 b 为基的数系表示：

$$p = r_k b^k + r_{k-1} b^{k-1} + \cdots + r_1 b + r_0$$

代数中元素的运算可归结为基底元素间的运算。如果以复数为“基”，是否可以在复平面表示所有图像呢?在这种情况下如何定义图像的代数运算?以及将此类运算应用于数字图像分存问题会带来什么好处呢？这些都是本文要讨论的问题。

2 复整数基和复平面上数的表示

众所周知，复数的出现不但对于数学本身的发展有着极其重要的意义，同时也为信号分析、不恰当积分、应用数学等领域提供了重要的理论依据[3]。以复数为“基”，在复平面上表示图像，会是一个有意思的问题。下面将首先讨论一下以复数为基底的数的表示问题。

设 x,y 为实整数，则 $Z=x+\mathrm{i}y$ 称为高斯整数。若选定 b 为复数基，且高斯整数可写成 $Z=\sum_{j=0}^{k} r_j b^j$，则称 Z 在复数基 b 下是可表示的。在 Z 的表示中，如果由所有允许的 r_j 组成的集合能形成模 b 的完全剩余类，便可以把整数基之下表示复数的标准算法推广到复数基的情形，例如 $b=-1+\mathrm{i}$，数字符号 $r_j\in S=\{0,1\}$，那么，就可以成功地表示所有复数(不只限于高斯整数)。其中能表示所有的复数的基，称为恰当基，否则称为非恰当基。当$b=1-\mathrm{i}$时，由于不是所有的复数都能得到表示，所以 $b=1-\mathrm{i}$ 为非恰当基[9]。如果给定高斯整数 $P_0+\mathrm{i}Q_0$，那么什么样的复数基 $b=\xi+\mathrm{i}\eta$ 是可用的(其中 ξ,η 是不为零的整数)是值得研究的。

事实上，高斯早年已经证明了，如果$(\xi,\eta)=1$，即 ξ 与 η 互素，那么 $S=\{0,1,2,\cdots,\xi^2+\eta^2-1\}$就形成了模 $b=\xi+\mathrm{i}\eta$ 的完全剩余类[10]。为了使得在$b=\xi+\mathrm{i}\eta$之下所能表示的高斯整数尽可能多(未必全部)，自然应该取 $\eta=\pm1$，于是，在这种情况下，由于复数基应选择为 $\xi\pm\mathrm{i}$，因而，数字符号集合为$S=\{0,1,2,\cdots,\xi^2\}$；另一方面，本文规定了 $S=\{0,1\}$，这就是说，限定 $\xi=\pm1$，于是可考虑的复数基仅有以下 4 个：$1+\mathrm{i}$，$1-\mathrm{i}$，$-1+\mathrm{i}$，$-1-\mathrm{i}$。进一步，在上述 4 个复数基中，互相共轭的复数$-1+\mathrm{i}$与$-1-\mathrm{i}$是恰当基，$1+\mathrm{i}$ 与 $1-\mathrm{i}$ 不是恰当基[2]，但可将这 4 个基统一记作 $b=\xi+\mathrm{i}\eta$，其中 $\xi,\eta=\pm1$。

值得注意的是，数字符号集合 S，如果按照上面“b 进制”的说法，那么它就是模 b 的完全剩余类。事实上，当取 b 为复数的时候，势必同时要对数字符号集合 S 作出某种规定。基于数字计算机的特点，本文规定 $S=\{0,1\}$。这里可先取 $r_j\in(0,1)$，$b=-1+\mathrm{i}$ 作为例子来说明这个问题(见表 1)。

表 1 以 $b=-1+\mathrm{i}$ 为基的整数表示

Decimal	Binary	With base $b=-1+\mathrm{i}$
0	0	0
1	1	1
2	10	$-1+\mathrm{i}$
3	11	i
4	100	$-2\mathrm{i}$
5	101	$1-2\mathrm{i}$
6	110	$-1-\mathrm{i}$
7	111	$-\mathrm{i}$
8	1000	$2+2\mathrm{i}$
9	1001	$3+2\mathrm{i}$
10	1010	$1+3\mathrm{i}$
11	1011	$2+3\mathrm{i}$
⋮	⋮	⋮

3 图像和复平面上点的映射算法

基于以上的讨论，这一节，将根据选定的复数基来提出图像到复平面上对应点的映射算法。若无特别说明，就认为所有的讨论皆在 $b=-1+\mathrm{i}$ 之下进行。而且，数字符号集合 $S=\{0,1\}$。事实上，如果将一幅图像转化为平面上的一个点，则许多图像间的关系问题可以转化为平面几何问题来处理。其实，这种映射关系归根到底是 0-1 序列到复平面上对应点的映射，因此，其不仅适用于图像，同时也适用于文字、声音、视频等其他媒体。

3.1 图像到复平面上对应点的映射算法

图像到复平面上对应点的映射算法如下：

首先,将图像从二维信号变换到一维空间的0-1序列。这种变换有很多方式(如图 1 所示)。令图像为 $I=f(x,y)$,则函数 $G:I\to N$ 为选择的变换方式。

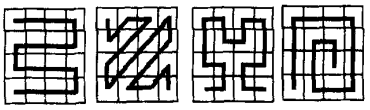


图 1　图像的线形化

如果已知在 $b=-1+\mathbf{i}$ 之下的一个 0-1 代码序列 $e_Ne_{N-1}\cdots e_2e_1e_0$,那么要回答它代表哪个高斯整数,这是容易的,因为,如果令

$$(\mathbf{i}-1)^k=r_k+\mathbf{i}s_k$$

在这样的记法之下,当 $k=0$ 时,自然有 $r_0=1$,$s_0=0$,那么由

$$(\mathbf{i}-1)^k=(\mathbf{i}-1)(r_{k-1}+\mathbf{i}s_{k-1})$$

可知

$$r_k+\mathbf{i}s_k=-r_{k-1}-s_{k-1}+\mathbf{i}(r_{k-1}-s_{k-1})$$

于是有

$$s_{k+1}=r_k-s_k,r_{k+1}=-r_k-s_k,r_0=1,s_0=0$$
$$k=0,1,2,\cdots \tag{1}$$

最后可以得到

$$\sum_{j=0}^{N}e_jr_j=P_0,\quad \sum_{j=1}^{N}e_js_j=Q_0$$

同理,对于一般情形,

$$r_{k+1}=\xi r_k-\eta s_k,s_{k+1}=\eta r_k+\xi s_k$$
$$r_0=1,s_0=0,k=0,1,2,\cdots$$

3.2　复平面上的点到图像的映射算法

给定复数 $P_0+\mathbf{i}Q_0$,在复数基 b 下,假设它的0-1序列写为 $e_Ne_{N-1}\cdots e_2e_1e_0$,其任务是确定 $\{e_j\}$,$j=0,1,2,\cdots,N-1,N$。由于

$$P_0+\mathbf{i}Q_0=e_Nb^N+e_{N-1}b^{N-1}+\cdots e_2b^2+e_1b^1+e_0b^0$$

换个写法,则为

$$P_0+\mathbf{i}Q_0=(-1+\mathbf{i})(P_1+\mathbf{i}Q_1)+e_0$$
$$=-P_1-Q_1+(P_1+Q_1)\mathbf{i}+e_0$$

其中 $e_0\in S=\{0,1\}$,由此可推得

$$P_0=-P_1-Q_1+e_0,Q_0=P_1-Q_1$$

从而得到以下递推算法:

$$P_{k+1}=\frac{Q_k-P_k+e_k}{2}$$
$$Q_{k+1}=\frac{-Q_k-P_k+e_k}{2},k=0,1,2,\cdots \tag{2}$$
$$e_k=|(P_k-Q_k)\bmod 2|$$

也就是说,如果 P_k,Q_k 奇偶性相同,则取 $e_k=0$;如果 P_k,Q_k 奇偶性相异,则取 $e_k=1$。

由计算的结果可依序排列得到 $e_Ne_{N-1}\cdots e_2e_1e_0$。

这就是说,当给定一个复数 $P_0+\mathbf{i}Q_0$ 时,通过递推式(式(2))即可得到它的 0-1 码序列。注意,它是在 $b=-1+\mathbf{i}$ 之下(将来它就是一个密钥)的表示,复数基 b 还可以另外选取,递推式也将随之做一点改变。

3.3　运算定义与示例

对于图像,一个 64×64 局部 Lena 图,将是一个长度为 64×64×8 bit 的 0-1 序列,它对应的复平面上的点如图 2 所示,可见,由于其实部和虚部都是大整数,因此,图像到点的映射运算需要用到大整数计算。一般地,可以做如下定义:函数 $G(x):x\to N$ 为信息媒体编码到二进制序列的变换函数,$G^{-1}(N):N\to x$ 为其逆变换;函数 $F_b(N):N\to(p,q)$ 定义为二进制序列到复平面上点的映射过程,$F_b^{-1}(p,q):(p,q)\to N$ 为其逆变换;函数 $T(x)=F_b(G(x)):x\to(p,q)$ 定义为信息媒体编码到复数的变换。

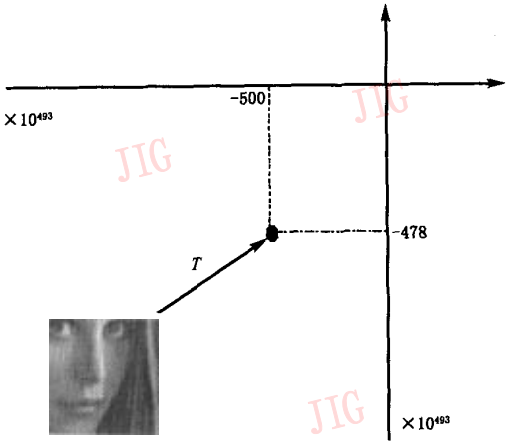


图 2　图像在复平面上的表示

对应地,将图像映射为复平面上的点后,就可以按照以上的规定来定义复平面上图像的运算。图像 I_A 和 I_B 之间的运算可以定义如下:

$$I_A\hat{+}I_B=T^{-1}(T(I_A)+T(I_B))=T^{-1}((p_A+p_B),(q_A+q_B))=I_C$$
$$I_A\hat{-}I_B=T^{-1}(T(I_A)-T(I_B))=T^{-1}((p_A-p_B),(q_A-q_B))=I_C$$
$$I_A\hat{\times}I_B=T^{-1}(T(I_A)\times T(I_B))=T^{-1}((p_A\times p_B),(q_A\times q_B))=I_C$$
$$I_A\hat{\div}I_B=T^{-1}(T(I_A)\div T(I_B))=T^{-1}((p_A\div p_B),(q_A\div q_B))=I_C$$

其中,$\hat{+},\hat{-},\hat{\times},\hat{\div}$ 是复平面上的加、减、乘、除。

图像 I_A 的共轭图像可定义为

$$I_A^*=T^{-1}(p_A,-q_A)$$

图像 I_A 的反图像可定义为

$$-I_A = T^{-1}(-p_A, -q_A)$$

这样，图像的加法和减法就等价于向量的加法和减法，也服从于平行四边形法则。向量变换（旋转和伸缩）就是乘、除法的几何意义。例如和 i 相乘，相当于逆时针旋转 90°。$i^2=-1$ 的几何解释即是连续旋转两个 90°。代数式 $(-1)\cdot(-1)=+1$，则可以解释成两次 180°的翻转。

根据以上的定义，以一系列 32×32 的图像做了下列实验。图版 I 图 1 为不同图像的加法运算结果。图版 I 图 2 为图像的共轭图像和反图像；其中，图版 I 图 2(b)是图 2(a)的共轭图像，图 2(d)是图 2(c)的共轭图像，图 2(f)是图 2(e)的共轭图像，图 2(g)是图 2(e)的反图像。结合以上论述和实验结果，可以得到以下结论：

(1)任何一幅图像，都能对应复平面上的一个点；不同的数字图像则对应复平面上不同的点；

(2)可将图像运算关系问题转化为几何问题来解决；

(3)对图像求其共轭和反图像有加密效果。

4 图像复数表示在秘密分存中的应用

根据本文中图像的加、减法定义，图像的加、减法等价于复平面上向量的加法和减法，并服从平行四边形法则。这样很容易想到利用这一点建立可视秘密分存的(2,3)门限方案，同时利用实部和虚部分别对应不同的图像组合来建立图像分存的(m,n)门限方案。也就是说，可换一种思路来考虑如今图像分存中的一些问题。

如上所述，在 R^2 向量空间中，任何一个向量都可以是其他两个向量的线性组合。如图 3 所示，令 P_s（下角 s 代表 secret，下同）是秘密图像中对应的点，P_1,P_2,P_3 是 3 幅公开图像中对应的点，P_1,P_2,P_3 两两无关，可得

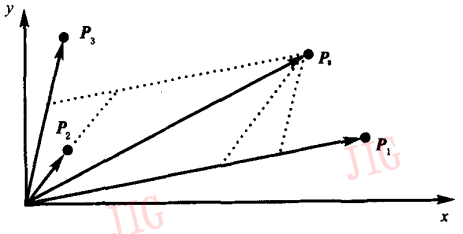


图 3 向量的线性组合分存方案

$$\lambda_1 P_1 + \lambda_2 P_2 = P_s$$
$$\lambda_3 P_1 + \lambda_4 P_3 = P_s$$
$$\lambda_5 P_2 + \lambda_6 P_3 = P_s$$

即 P_1,P_2,P_3 中的任何两两组合就可以得到 P_s，如果少于两点，则 P_s 不能被表示，λ_i 可记为密钥，这便是典型的(2,3)门限分存方案[6]。同样可以在三维空间或更广阔的范围寻找类似的关系，此处不再赘述。

进一步，若考虑将点 P_s 的坐标(x_s,y_s)当作一个复数的实部和虚部(P,Q)，则(P,Q)也是两个大整数，如果使 $M=\{P,Q\}$，并用 P_{11}和 P_{12}来分别表示与 P 和 Q 对应的复平面上的点，则有

$$T(M)=T(P)\rightarrow(x,y)\rightarrow P_{11}$$
$$T(M)=T(Q)\rightarrow(x_2,y_2)\rightarrow P_{12}$$

即 P_{11}和 P_{12}也对应两幅图像，同样 P_2,P_3 也可以做类似处理，那么，以上方案可以定义为

$$f(P_s):(P_{11}\cap P_{12})\oplus(P_{21}\cap P_{22})\cup(P_{11}\cap P_{12})\oplus(P_{31}\cap P_{32})\cup(P_{31}\cap P_{32})\oplus(P_{21}\cap P_{22})\rightarrow P_s$$

可以叫做类(4,6)门限方案，如图 4 所示。

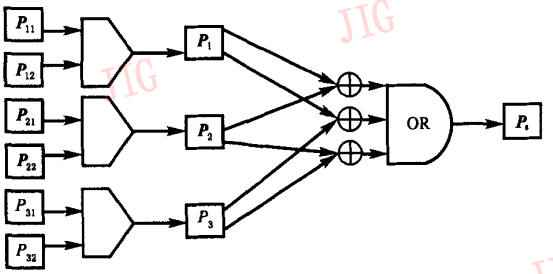


图 4 类(4,6)门限方案

假设图版 I 图 3(a)是秘密图像 A，选择 3 幅公开图像 B_i(64×64×24b)作为影子图像（如图版 I 图 3(c)所示）。秘密图像分存时，首先将所有的图像映射为复平面上的点，然后使用上述的(2,3)门限方案就可以计算图像对应各点向量间的关系，并记录为密钥 λ_i。图版 I 图 3(b)所示即为由不同的影子图像组合而重构的保密图像。图版 I 图 4 则是用类(4,6)门限方案进行图像秘密分存的例子。在影子图像的选择中，有 256 级灰度图像、RGB 彩色图像以及黑白图像，它们都可以用来测试算法的效果。

5 结 论

本文首先利用位值制记数法的基本思想来在复

平面上表示图像,以便换一个角度考虑传统图像处理中的一些问题,同时给出了图像和复平面上点的映射算法,并用复数运算来定义图像和图像间的"加"、"减"、"乘"、"共轭"等运算关系,并针对信息的可视分存问题,提出了一种基于数系的新方法;最后通过不同类型的数据对算法进行了有效的论证。实验结果表明,用毫不相干的影子图像来分存秘密信息不仅能够达到保密的目的,并能隐藏是否正在通信的的事实。实践证明,本方法也可用于其他图像伪装方案[11]。

参 考 文 献

1 Shamir A. How to share a secret[J]. Communications of the ACM, 1979,**24**(11):612～613.

2 Blakeley G R. Safeguarding cryptographic keys [A]. In: Proceedings of AFIPS National Computer Conference [C], Boston, New Jersey, USA, 1979,**48**:313～317.

3 Simmons G J. An introduction to shared secret and/or shared control scheme and their application[A]. In: Simmons G J edi. Contemporary Cryptology, The Science of Information Integrity [C], IEEE Press, 1992:441～497.

4 Naor M, Shamir A. Visual cryptography[A]. In: Advances in Cryptology—EUROCRYPT'94 Lecture Notes in Computer Science[C], Perugia, Italy, 1994,**950**:1～12.

5 Yue Tai-wen, Chiang Suchen. A neural network approach for visual cryptograpgy[A]. In: Proceedings of IEEE-INNS-ENNS International Joint Conference on Neural Networks[C], Como, Italy, 2000,**5**: 5494.

6 Chang Chin-chen, Tsai Chwei-shyong, Chen Tung-shou. A new scheme for sharing secret color images in computer network[A]. In: Proceedings of Seventh International Conference on Parallel and Distributed Systems[C], Iwate, Japan,2000:21～27.

7 Chang Chin-chen, Yu Tai-xing. Sharing a secret gray image in multiple images[A]. In: Proceedings of the first symposium on cyber worlds[C], Tokyo, Japan, 2002:230～237.

8 Kenneth R Cattleman 著. 朱志刚,林学闻,石定机译. 数字图像处理[M]. 北京:电子工业出版社,1999.

9 齐东旭. 分形及其计算机生成[M]. 北京:科学出版社,1994.

10 Katai I, Szabo J. Canonical number system for complex integers [J]. Acta Science Mathematics, 1975,**37**:255～260.

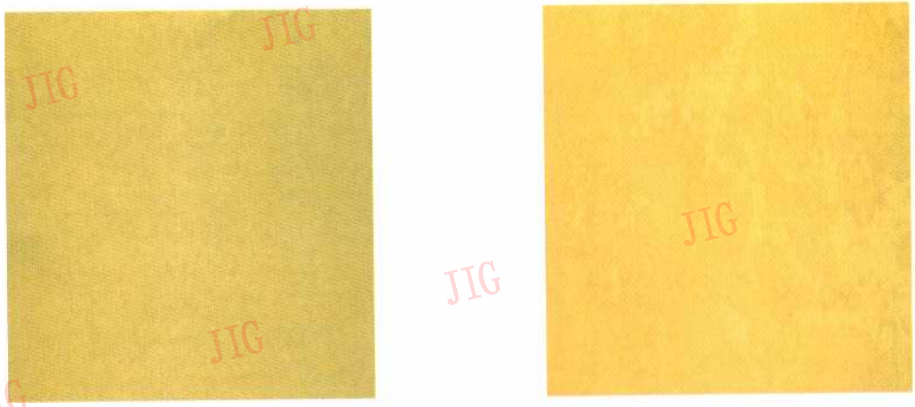
11 Sun Wei, Yang zhihua, Qi Dongxu. Number system based scheme for multimedia steganography[A]. In: Proceedings of 8th International conferences on CAD/Graphics [C], Macao, China, 2003:93～98.

孙　伟　1972 年生,2004 年于中山大学获得工学博士学位。主要研究方向为计算机图形学和网络环境下的信息安全。已发表学术论文 20 余篇。

E-mail:Wellsun2002@yahoo.com.cn

杨志华　1964 年生,1995 年于湖南大学获得工学硕士学位,现为中山大学计算机软件与理论专业博士生。主要研究方向为计算机图形学和网络环境下的信息安全。

齐东旭　教授,博士生导师。主要研究领域为数值分析、计算机辅助几何设计、计算机图形学、计算机动画、数字图像压缩和数字图像的信息安全处理等。发表论文 130 余篇,出版专著 5 部。



(a) 单色瓷砖　　(b) 纹理瓷砖

图1　实验瓷砖图像

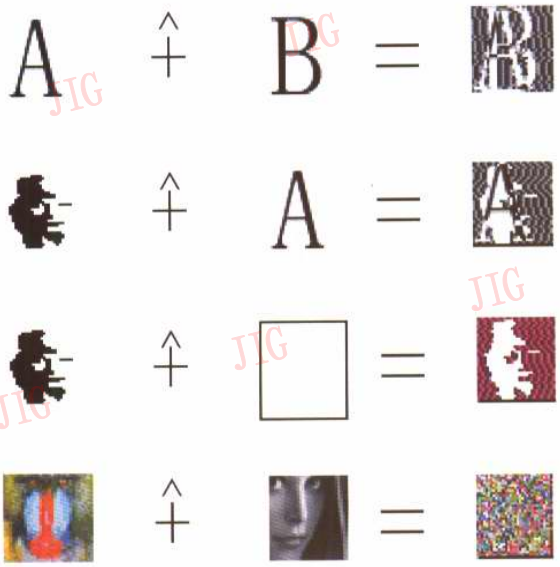
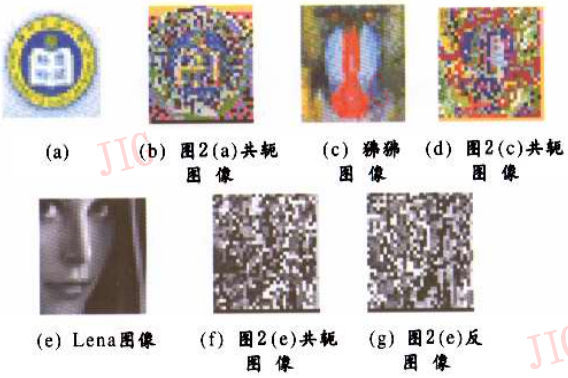


图1　图像加法运算



(a)　(b) 图2(a)共轭图像　(c) 狒狒图像　(d) 图2(c)共轭图像

(e) Lena图像　(f) 图2(e)共轭图像　(g) 图2(e)反图像

图2　共轭图像和反图像

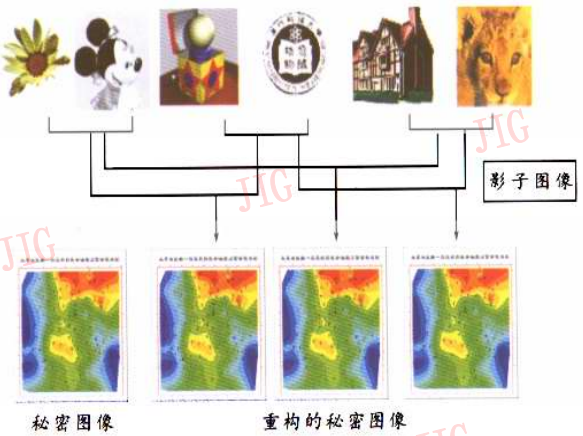
(a) 秘密图像 airplane(64×64)　(1)　(2)　(3)

(b) 重构的秘密图像

影子图像 B_1 Lena(64×64)　影子图像 B_2 Baboon(64×64)　影子图像 B_3 Peppers(64×64)

(c)

图3　(2,3)门限方案



秘密图像　重构的秘密图像

图4　类(4,6)门限方案