

(12) 发明专利

(10) 授权公告号 CN 101010905 B

(45) 授权公告日 2010.08.25

(21) 申请号 200580029820.2

(51) Int. Cl.

(22) 申请日 2005.08.31

H04L 9/08(2006.01)

(30) 优先权数据

H04N 1/44(2006.01)

259633/2004 2004.09.07 JP

(56) 对比文件

(85) PCT申请进入国家阶段日

JP 特开 2003-324418 A, 2003.11.14, 说明书 [0048]、图 8.

2007.03.06

CN 1450495 A, 2003.10.22, 全文.

(86) PCT申请的申请数据

CN 1204109 A, 全文.

PCT/JP2005/016364 2005.08.31

US 6473859 B1, 2002.10.29, 全文.

(87) PCT申请的公布数据

审查员 王澍

W02006/028103 EN 2006.03.16

(73) 专利权人 佳能株式会社

地址 日本东京

(72) 发明人 林淳一

(74) 专利代理机构 中国国际贸易促进委员会专

利商标事务所 11038

代理人 马浩

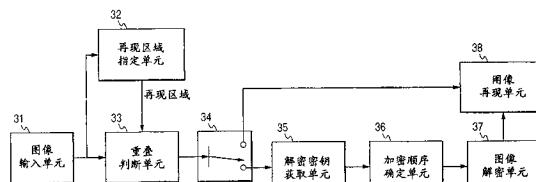
权利要求书 1 页 说明书 12 页 附图 13 页

(54) 发明名称

信息处理方法、信息处理装置、用来实现该信息处理方法的计算机程序、及存储该计算机程序的计算机可读存储介质

(57) 摘要

本发明的目的在于提供适当地允许对图像数据的部分区域的加密和解密的技术，对于该图像数据已经施加局部加密和多重加密。更具体地说，在图像数据中的预定图像区域由再现区域指定单元获取，所获取的图像区域和被加密的加密区域的重叠区域由重叠判断单元计算，与计算的重叠区域相对应的密钥信息由解密密钥获取单元获取，及与重叠区域相对应的图像数据由解密密钥获取单元获取，并且与重叠区域相对应的图像数据由图像解密单元通过使用获取的密钥信息经受加密和解密。



1. 一种图像再现方法,通过其再现加密图像数据,所述方法包括:

区域获取步骤,获取在图像数据中的预定图像区域;

区域计算步骤,计算所获取的预定图像区域和被加密的加密区域的重叠区域;

密钥信息获取步骤,获取与所述区域计算步骤中计算的重叠区域相对应的密钥信息;及

解密步骤,通过使用在所述密钥信息获取步骤中获取的密钥信息,对与所述重叠区域相对应的图像数据执行解密处理。

2. 根据权利要求 1 所述的图像再现方法,其中,

所述加密图像数据至少具有通过使用第一密钥信息加密的第一加密区域、和通过使用第二密钥信息加密的第二加密区域,并且

所述区域计算步骤适于至少计算作为第一加密区域和所述预定图像区域的交集的第一重叠区域以及作为第二加密区域和所述预定图像区域的交集的第二重叠区域。

3. 根据权利要求 2 所述的图像再现方法,其中所述密钥信息获取步骤适于至少获取与第一重叠区域相对应的第一密钥信息和与第二重叠区域相对应的第二密钥信息。

4. 根据权利要求 3 所述的图像再现方法,还包括:加密顺序确定步骤,确定关于第一加密区域和第二加密区域的加密顺序,

其中所述解密步骤适于根据在所述加密顺序确定步骤中确定的加密顺序执行解密处理。

5. 一种再现加密图像数据的图像再现装置,包括:

区域获取单元,适于获取在图像数据中的预定图像区域;

区域计算单元,适于计算所获取的预定图像区域和被加密的加密区域的重叠区域;

密钥信息获取单元,适于获取与所述区域计算单元计算的重叠区域相对应的密钥信息;及

解密单元,适于通过使用由所述密钥信息获取单元获取的密钥信息,对与所述重叠区域相对应的图像数据执行解密处理。

6. 根据权利要求 5 所述的图像再现装置,其中,

所述加密图像数据至少具有通过使用第一密钥信息加密的第一加密区域、和通过使用第二密钥信息加密的第二加密区域,并且

所述区域计算单元适于至少计算作为第一加密区域和所述预定图像区域的交集的第一重叠区域以及作为第二加密区域和所述预定图像区域的交集的第二重叠区域。

7. 根据权利要求 6 所述的图像再现装置,其中所述密钥信息获取单元适于至少获取与第一重叠区域相对应的第一密钥信息和与第二重叠区域相对应的第二密钥信息。

8. 根据权利要求 7 所述的图像再现装置,还包括:加密顺序确定单元,适于确定关于第一加密区域和第二加密区域的加密顺序,

其中所述解密单元适于根据由所述加密顺序确定单元确定的加密顺序执行解密处理。

信息处理方法、信息处理装置、用来实现该信息处理方法的计算机程序、及存储该计算机程序的计算机可读存储介质

技术领域

[0001] 本发明涉及图像数据的加密和解密技术。

背景技术

[0002] 传统上,为了图像数据等的访问控制,加密和加扰图像数据。更具体地说,图像数据通过使用加密密钥预先加密,由此只有具有与相关加密密钥相对应的解密密钥的人员才能正确地再现被加密的图像数据。

[0003] 这里,局部加密已知为加密图像数据的方法之一。更明确地说,局部加密是不加密全部图像数据而是选择并加密图像数据的部分区域的技术(例如,见美国专利No. 6,473,859)。

[0004] 而且,局部解密已知为解密加密图像数据的方法之一。更明确地说,局部解密是不解密全部加密图像数据而是选择并解密加密图像数据的部分区域的技术(例如,参见公开的美国专利申请 2003/0190042)。

[0005] 此外,加密图像数据若干次的多重加密是已知的。这里,多重加密是当加密图像数据被进一步加密时使用的技。

[0006] 就是说,通过适当地使用局部加密、局部解密或多重加密,有可能实现图像数据的灵活访问控制。

[0007] 然而,在过去,局部加密、局部解密及多重加密没有被组合地使用,并且没有公开任何的在局部加密、局部解密及多重加密被适当组合并应用于图像数据的情况下再现图像的方法。

[0008] 顺便说明,在其中按一定加密顺序受到多重加密的图像数据被解密的情况下,必须按与以上加密顺序相反的顺序执行解密。在该情况下,预料到有如下问题。就是说,如果部分加密和多重加密图像数据经受局部解密,则不可能指定相对区域的哪一个已经经受多重加密。因而,有可能对于解密不必要的密钥被不必要地获得。另外,不可能相对于将要被解密并且再现的区域指定解密顺序。因而,有可能不能执行局部解密,从而经受多重解密的全部区域被不必要地解密。

发明内容

[0009] 考虑到以上传统问题而完成本发明,并且其目的在于,提供用来适当地允许执行已经经受局部加密和多重加密的图像数据的局部解密的技术。

[0010] 此外,为了实现以上目的,本发明的特征在于包括:区域获取步骤,获取在图像数据中的预定图像区域;区域计算步骤,计算获取的预定图像区域和加密的加密区域的重叠区域;密钥信息获取步骤,获取与在区域计算步骤中计算的重叠区域相对应的密钥信息;及解密步骤,通过使用在密钥信息获取步骤中获取的密钥信息,对于与重叠区域相对应的图像数据执行解密处理。

[0011] 本发明的其它目的、特性及优点由联系附图所做的如下详细描述而显而易见。

附图说明

- [0012] 图 1 是示意图,表示根据本发明实施例的系统的整个构造;
- [0013] 图 2 表示在根据本实施例执行加密处理的情况下 GUI(图形用户界面)屏幕的例子;
- [0014] 图 3 是方块图,表示根据本实施例的主计算机的构造;
- [0015] 图 4 是方块图,表示根据本实施例的图像加密处理单元的构造;
- [0016] 图 5A、5B、5C、5D、5E 及 5F 用来解释根据本实施例的图像区域指定;
- [0017] 图 6 是流程图,表示根据本实施例的图像加密处理;
- [0018] 图 7 用来解释根据本实施例的密钥信息的记录方法;
- [0019] 图 8 是方块图,用来解释图像解密处理单元的构造;
- [0020] 图 9A、9B 及 9C 用来解释根据本实施例的解密相关信息;
- [0021] 图 10A、10B 及 10C 用来解释根据本实施例的重叠区域的例子;
- [0022] 图 11 是流程图,表示根据本实施例的图像解密处理;
- [0023] 图 12 是方块图,用来解释根据本实施例的图像解密单元的构造;
- [0024] 图 13 是流程图,表示根据本实施例的图像解密处理;及
- [0025] 图 14A、14B、14C、14D 及 14E 用来解释根据本实施例的图像再现的例子。

具体实施方式

- [0026] (整个构造的解释)

[0027] 图 1 表示根据本发明实施例的系统的整个构造的例子。在图 1 中,图像加密装置 91 通过使用预定密钥执行对于通过扫描仪、数字摄像机等输入的图像数据的加密处理。密钥服务器 92 响应于预定密钥信息获取信息,传送在密钥 DB(数据库)93 中存储的和解密所述加密图像数据必需的密钥信息。图像传送服务器 94 响应于预定图像数据获取请求,传送在图像 DB 95 中存储的图像数据。图像再现装置(或图像查看器)96 接收图像数据,解密接收图像数据的加密,及再现图像数据。这里,在图 1 中,功能方块 91 至 96 通过诸如因特网 97 之类的网络相互连接,借此在这些方块 91 至 96 中可交换各种数据。顺便说明,功能方块 91 至 96 的每一个可以是诸如普通个人计算机等之类的通用装置。然后,下文将解释系统的实际处理。

[0028] 图像加密装置 91 通过使用预定密钥信息对于所希望的图像数据执行压缩处理和加密处理,并且把压缩和加密的图像数据传输到图像传送服务器 94。同时,图像加密装置 91 把在加密处理中使用的密钥信息传输到密钥服务器 92。然后,密钥服务器 92 把接收的密钥信息与用来指定对应图像数据的信息(例如,图像 ID(标识))一起登记在密钥 DB 93 中。

[0029] 图像查看者(就是说,观看图像的人员)请求图像传送服务器 94 传送所希望的图像数据,并且然后通过使用图像再现装置 96 接收图像数据。然而,在该情况下,由于所希望的图像数据已经加密,所以图像查看者还请求密钥服务器 92 产生用来解密所述加密图像数据的密钥信息。在这时,例如,密钥服务器 92 可以执行适当的验证处理以判断是否能够

把密钥信息传送到相关查看者，并且只有在其中判断能够传送密钥信息的情况下才传送密钥信息。因而，密钥信息通过因特网 97 从密钥服务器 92 传输到图像再现装置 96，加密图像数据通过使用传输的密钥信息在图像再现装置 96 中被解密，及图像数据最后被再现。

[0030] 顺便说明，在对图像加密装置 91 执行的加密处理的详细解释之前，参照图 2 将解释图像加密处理和在根据本实施例的图像再现处理中的操作屏幕（窗口）的例子。

[0031] 如图 2 中所示，空白栏 102 用来指定包括待加密或再现的图像数据的输入文件，空白栏 103 用来指定包括加密必需的密钥信息的密钥文件，及空白栏 104 用来指定包括作为加密结果或再现结果的图像数据的输出文件，它们排列在窗口 101 的上侧。这里，在空白栏 102、103 及 104 的每一个中的项目可以借助于稍后描述的键盘 1115（图 3）的使用通过直接输入文件名而指定，或者通过点击排列在每个空白栏右边上的按钮从显示的文件浏览器中选择。在空白栏 102 处指定的文件中包括的图像数据被显示在图像浏览器 105 上。在该实施例中，当图像加密处理被执行时，所需要的打算被隐藏的区域通过使用鼠标等从在图像浏览器 105 上显示的图像数据中选择，借此只有被选择区域可被加密。同样，当图像再现处理被执行时，所需要的打算再现的区域通过使用鼠标等被选择，借此只有被选择的区域可被再现。在图 2 中，矩形 106 表示待选择区域的例子。典型地，在其中所需要的再现区域通过在图像再现中使用矩形 106 指定的情况下，难以确定应该指定在图像中的哪个区域，因为根本不显示相关图像的内容。在这样一种情况下，例如，有可能以低图像质量和低分辨率在图像浏览器 105 中预先显示图像的内容，并且然后对于通过使用矩形 106 选择的区域再现（显示）高质量和高分辨率图像。此外，在其中分辨率水平、层、分量或其组合被指定、而不是图像数据的空间区域被指定的情况下，分辨率水平的索引、层的索引、及 / 或分量的索引分别输入到空白栏 1010、空白栏 1011 及 / 或空白栏 1012。

[0032] 然后，在所希望的区域按以上选择之后，如果加密按钮 107 被按下，则对与选择区域相对应的图像数据执行加密处理。除此之外，如果再现按钮 109 被按下，则对选择区域执行解密处理，借此图像数据被再现。就是说，在加密处理或解密处理被执行之后，重新绘制在图像浏览器 105 中被执行，借此经受加密处理的图像数据或经受解密处理的图像数据被显示在图像浏览器 105 中。在该实施例中，具体地说，在加密处理通过按下加密按钮 107 被执行之后，新指定一个与矩形 106 不同的矩形区域（或矩形），并且加密按钮 107 被再次按下，借此有可能执行加密处理多次。这样，在加密处理执行多次之后，结束按钮 108 被最终按下，从而所述图像数据被记录在通过空白栏 104 指定的文件中。

[0033] 顺便说明，在图 2 中表示的窗口仅用于可应用于本发明的一个例子。就是说，显然本发明不限于此。

[0034] 以后，参照图 3 将解释可应用在本发明实施例中的主计算机。就是说，图 3 是方块图，它表示起根据实施例的图像加密装置和图像再现装置作用的主计算机的基本构造，并且也表示在主计算机与其外围设备之间的关系。在图 3 中，主计算机 111，例如为流行个人计算机，可通过 I/F（接口）1117 从扫描仪 1116 输入图像数据，并且然后编辑和存储输入的图像数据。此外，主计算机 111 可通过使用 NIC（网络接口卡）1110 或调制解调器 1112 经因特网等分配所获取的图像数据。这里，应该注意，各种指令等等通过鼠标 1114 和键盘 1115 从用户输入。在主计算机 111 中，以后描述的功能方块通过总线 1118 相互连接，借此可交换各种数据。

[0035] 在图 3 中,附图标记 112 表示可显示来自主计算机 111 的各种信息的监视器。

[0036] 附图标记 113 表示 CPU, 可控制在主计算机 111 中的相应功能方块的操作并且执行加载到以后描述的 RAM 115 中的程序。附图标记 114 表示 ROM, BIOS 和引导程序已经存储在其中。附图标记 115 表示 RAM, 待处理的程序和图像数据临时存储在其中以被 CPU 113 处理。除此之外, 用来使 CPU 113 执行以后描述的各种处理的程序加载到 RAM 115 中。

[0037] 附图标记 116 表示用来存储 OS(操作系统)和待传输到 RAM 等的程序的 HD(硬盘)。此外, 在主计算机 111 在操作时, HD 116 用来存储和读取图像数据。附图标记 117 表示可从是外部存储介质的 CD-ROM(或 CD-R)读取数据和 / 或向其写入数据的 CD-ROM 驱动器。

[0038] 附图标记 118 表示可像 CD-ROM 驱动器 117 那样从软盘读取数据和 / 或向其写入数据的 FD 驱动器。此外, 附图标记 119 表示可像 CD-ROM 驱动器 117 那样从 DVD-ROM 读取数据并且从 DVD-RAM 读取数据和 / 或向其写入数据的 DVD-ROM(或 DVD-RAM)驱动器。顺便说明, 在其中图像编辑程序存储在 CD-ROM、软盘、DVD-ROM 等中的情况下, 相关程序一次安装到 HD 116 中, 并且安装程序然后根据需要传输到 RAM 115。

[0039] 附图标记 1117 表示 I/F, 该 I/F 把扫描仪 1116 与总线 1118 相接合, 从而从扫描仪 1116 输入的图像数据可传输到在主计算机 111 中的 HD 116 和 RAM 115。

[0040] 附图标记 1111 表示 I/F, 该 I/F 把 NIC 1110 与总线 1118 相接合, 从而在主计算机 111 中的 RAM 115、HD 116、CD-ROM 驱动器 117、FD 驱动器 118、DVD-ROM 驱动器 119 等中存储的图像数据可传输到 NIC 1110。就是说, 主计算机 111 通过 I/F 1111 向因特网传输数据 / 从其接收数据。

[0041] 附图标记 1113 表示把鼠标 1114 和键盘 1115 与主计算机 111 接合的 I/F。因而, 各种指令通过 I/F 1113 从鼠标 1114 和键盘 1115 输入到主计算机 111 的 CPU 113。

[0042] (图像加密处理)

[0043] 图 4 是方块图, 用来解释根据实施例的图像加密处理功能和用来实现图像加密处理功能的方法。在图 4 中, 附图标记 11 指示图像输入单元, 附图标记 12 指示加密区域指定单元, 附图标记 13 指示加密密钥指定单元, 附图标记 14 指示加密单元, 附图标记 15 指示切换单元, 及附图标记 16 指示图像输出单元。

[0044] 最初, 将解释图像输入单元 11 的功能。待加密的图像数据通过图像输入单元 11 输入到加密区域指定单元 12。

[0045] 更具体地说, 图像输入单元 11 读取在图 3 中表示的 ROM 114、RAM 115、HD 116、CD-ROM 驱动器 117、FD 驱动器 118、DVD-ROM 驱动器 119 等中预先存储的图像数据, 并且然后输入所读取的图像数据。可选择地, 图像输入单元 11 从因特网 97(图 1)通过调制解调器 1112 或 NIC 1110 接收图像数据, 并且然后使用接收的图像数据。另外, 图像输入单元 11 通过使用扫描仪 1116 等数字化被印刷在例如纸上的原件的图像, 并且然后使用数字化的图像数据。就是说, 在实施例中可应用任何输入源。此后, 通过图像输入单元 11 输入的图像数据一次存储在 RAM 115 中。

[0046] 这里, 为了简化如下解释, 假定图像数据已经由被 ISO(国际标准化组织)标准化的 JPEG(联合图像专家组)2000 系统压缩。然而, 本发明不限于此。就是说, 显然也可应用由另一种 JPEG 系统等压缩的图像数据和未压缩的图像数据。

[0047] 以后,将解释加密区域指定单元 12 的功能。就是说,加密区域指定单元 12 指定包括在输入图像数据中并打算加密的区域,并且把涉及指定区域的区域信息输出到加密单元 14。

[0048] 在该实施例中,假定由加密区域指定单元 12 指定的区域是图像的空间区域。然后,参照图 5A 至 5F 将解释在该实施例中指定的区域。

[0049] 图 5A 至 5F 用来解释根据实施例的图像区域指定的例子。在图 5A 至 5C 中,附图标记 121 指示整个图像,并且附图标记 122、123、124 及 125 分别指示指定的(待加密)区域。在该实施例中,单个矩形区域可被指定,如图 5A 中所示,单个任意成形区域可被指定,如图 5B 中所示,及另外多个区域可被指定,如图 5C 中所示。这里,应该注意,当浏览或参考在图 2 中表示的图像查看器 105 时,有可能使用户通过使用鼠标 1114 等指定这些区域。可选择地,也有可能自动地指定在 RAM 115、HD 116 等中预先登记的预定区域。

[0050] 顺便说明,作为待指定的区域的一个例子,在本实施例中指定图像的空间区域。然而,本发明不限于此。就是说,显然可指定各种图像数据的部分区域。例如,显然,在 JPEG 2000 系统的图像数据中,预定分量(区域 126)可被指定,如图 5D 中所示,预定分辨率水平(区域 127)可被指定,如图 5E 中所示,及预定层(区域 128)可被指定,如图 5F 中所示。这里,应该注意,这些区域的索引可以分别输入到在图 2 中表示的空白栏 1012、1010 及 1011。

[0051] 以后,将解释加密密钥指定单元 13 的功能。就是说,加密密钥指定单元 13 指定与同由加密区域指定单元 12 在以前阶段中指定的区域相关的区域信息相对应的密钥信息,并且然后输出所指定的密钥信息。

[0052] 在该实施例中,来自密钥 DB 93 中预先存储的密钥信息中的所希望的密钥信息被请求到密钥服务器 92,然后从密钥服务器 92 传输的密钥信息被指定。可选择地,有可能在加密密钥指定单元 13 中新产生密钥信息,并且指定所产生的密钥信息。在该情况下,产生的密钥信息与用来指定图像数据的信息(例如,图像 ID 等)一起登记在密钥服务器 92 中,从而能够在以后阶段用在图像解密单元中。在任何情况下,相对于由加密区域指定单元 12 指定的每个区域不同的密钥信息在加密密钥指定单元 13 中被指定。

[0053] 以后,将解释加密单元 14 的功能。就是说,图像数据、加密区域信息及密钥信息输入到加密单元 14。然后,在加密单元 14 中,只有来自输入图像数据中的与加密区域信息相对应的数据才通过使用由加密密钥指定单元 13 在以前阶段指定的密钥信息而经受加密处理。然后,加密图像数据从加密单元 14 输出。

[0054] 顺便说明,用于加密处理的加密算法在该实施例中没有明确地限制。就是说,各种加密算法可应用于本发明。例如,诸如 DES(数据加密标准)、AES(高级加密标准)等之类的共享密钥加密算法和诸如 RSA(Rivest Shamir Adleman)等之类的已公布密钥加密算法是可应用的。

[0055] 当按下在图 2 中表示的加密按钮 107 时,执行在加密单元 14 中的加密处理。然后,在执行加密处理之后,在图像查看器 105 中重新绘制加密图像(就是说,已经扰码所述指定区域的图像)。

[0056] 以后,将解释切换单元 15 的功能。更明确地说,切换单元 15 切换两种操作,就是说,一种是再次执行在加密区域指定单元 12 中的加密区域指定处理、在加密密钥指定单元 13 中的加密密钥指定处理、及在加密单元 14 中的加密,并且另一种是结束加密处理并且执

行在图像输出单元 16 中的图像输出处理。

[0057] 这里,应该注意,在切换单元 15 中的切换操作可由操作者通过在图 2 中表示的图像浏览器 105 执行。就是说,如果由用户指定新区域则切换单元 15 连接到加密区域指定单元 12 上,而如果结束按钮 108 由用户按下则切换单元 15 连接到图像输出单元 16 上。

[0058] 除此之外,例如,加密处理的预定次数被预先登记在 RAM 115、HD 116 等中,并且提供用来计数加密处理的次数和判断加密处理是否执行了与登记的预定数量相对应的次数的计数器。因而,有可能按照计数器判断加密处理的次数是否超过登记的预定数量而切换操作。更明确地说,例如,如果计数数量等于或小于登记的预定数量,则切换单元 15 连接到加密区域指定单元 12 上,而如果计数数量超过预定数量,则切换单元 15 连接到图像输出单元 16 上。

[0059] 在任何情况下,本发明不限于此。就是说,显然在切换单元 15 中的切换处理能以各种方法执行。

[0060] 随后,加密图像数据最终从图像输出单元 16 输出。在图像输出单元 16 中,图像数据传输到图像传送服务器 94,或者一次存储在诸如 RAM 115、HD 116、CD-ROM 驱动器 117、FD 驱动器 118、DVD-ROM 驱动器 119 等之类的存储介质中。

[0061] 图 6 是流程图,表示可应用于本实施例的图像加密处理。

[0062] 最初,在步骤 S21 中,输入图像数据。然后,在步骤 S22 中,指定预定加密区域。以后,在步骤 S23 中,指定与在步骤 S22 中指定的加密区域相对应的密钥信息。此后,在步骤 S24 中,与在步骤 S22 中指定的区域相对应的图像数据通过使用在步骤 S23 中指定的密钥信息经受加密处理。在加密处理执行之后,在步骤 S25 中判断整个加密处理是否结束。这里,如果判断加密处理应该继续,流程返回到步骤 S22。同时,如果在步骤 S25 中判断整个加密处理结束,则图像加密处理结束。

[0063] 如以上解释的那样,根据本实施例,有可能对于图像数据的预定区域执行加密处理多次。

[0064] 顺便说明,在该实施例中,作为在加密区域指定处理中指定的加密区域,每当执行加密区域指定处理时可指定不同区域。同样,作为在加密处理中使用的密钥信息,每当执行加密处理时可使用不同的密钥信息。

[0065] 因而,多个加密区域被指定,并且加密处理通过使用相对于每个加密区域不同的密钥信息而执行。在该情况下,为了在以后阶段在图像再现处理单元中正确地执行图像解密处理,在图像数据中必须记录哪个密钥信息对于哪个区域被使用。这里,参照图 7 将解释如何在该实施例中记录加密区域信息和密钥信息。

[0066] 图 7 用来解释根据实施例的区域信息和密钥信息的记录方法。附图标记 81 指示全部图像数据,附图标记 82 指示用来记录涉及图像数据的各种参数的首部信息,附图标记 83 指示实际图像数据,附图标记 84 指示加密相关信息,附图标记 85 指示第一加密相关信息,及附图标记 86 指示第二加密相关信息。这里,在该实施例中假定,第一加密处理首先执行,并且此后执行第二加密处理。

[0067] 如图 7 中所示,在该实施例中,加密顺序信息、加密区域信息及密钥信息被记录为图像数据的首部信息的一部分。此外,应该注意,第一加密相关信息 85 包括加密顺序信息 1、第一加密区域信息 Z1 及第一密钥信息 K1,并且第二加密相关信息 86 包括加密顺序信息

2、第二加密区域信息 Z2 及第二密钥信息 K2。

[0068] 在图 7 中表示的例子中, 初始对于由第一加密区域信息 Z1 指示的区域通过使用第一密钥信息 K1 执行加密处理作为第一加密处理, 并且以后对于由第二加密区域信息 Z2 指示的区域通过使用第二密钥信息 K2 执行加密处理作为第二加密处理。由于相关信息记录在首部信息 82 中, 所以有可能把在图像加密处理中通过使用哪个密钥对哪个区域执行加密处理通知给以后描述的图像再现处理单元。

[0069] 顺便说明, 指示第一密钥信息和第二密钥信息的标识符可以被记录为密钥信息。可选择地, 有可能通过使用与第一密钥信息和第二密钥信息不同的第三密钥信息加密第一密钥信息和第二密钥信息, 并且然后记录加密的第一密钥信息和加密的第二密钥信息。这里, 应该注意, 加密区域信息可以是允许知道加密区域位于图像数据中的哪部分的信息。例如, 加密区域信息可以是像素号或图像数据的坐标, 或者可以是当把图像数据划分成预定块时获取的块号。

[0070] 此外, 在该实施例中, 加密顺序信息、加密区域信息及密钥信息记录在图像数据中, 如图 7 中所示。然而, 显然本发明不限于此。例如, 加密顺序信息、加密区域信息及密钥信息可记录为与图像数据分离的其它数据, 并且然后在以后阶段传输到图像再现处理单元。

[0071] 除此之外, 在该实施例中假定, 在执行第一加密处理之后, 执行第二加密处理。然而, 不用说, 在执行第二加密处理之后, 可执行第三加密处理, 就是说, 可以执行 n 次多重加密处理。在这时, 通过第 n 次的加密而加密的第 n 次加密相关信息 (就是说, 加密顺序信息 n、加密区域信息 Zn 及密钥信息 Kn) 记录在首部信息 82 的加密相关信息 84 中。

[0072] (图像再现处理)

[0073] 图 8 是方块图, 用来解释根据实施例的图像再现处理功能和实现图像再现处理功能的方法。在图 8 中, 附图标记 31 指示图像输入单元, 附图标记 32 指示再现区域指定单元, 附图标记 33 指示重叠判断单元, 附图标记 34 指示切换单元, 附图标记 35 指示解密密钥获取单元, 附图标记 36 指示加密顺序确定单元, 附图标记 37 指示图像解密单元, 及附图标记 38 指示图像再现单元。

[0074] 最初, 将解释图像输入单元 31 的功能。就是说, 打算再现的图像数据输入到图像输入单元 31, 并且输入的图像数据从图像输入单元 31 输出到再现区域指定单元 32 和重叠判断单元 33。在该实施例中, 假定由在图 4 中表示的图像输出单元 16 输出的 (就是说, 加密的) 图像数据输入到图像输入单元 31。换句话说, 通过在执行第一加密处理之后执行第二加密处理而获取的图像数据输入到图像输入单元 31。

[0075] 接下来, 将解释再现区域指定单元 32 的功能。就是说, 在再现区域指定单元 32 中, 输入打算再现的图像数据, 指定在输入图像数据中所希望的再现区域 V, 及把指定的再现区域 V 输出到重叠判断单元 33。这里, 应该注意, 有可能使用户在浏览或参考在图 2 中表示的图像浏览器 105 时, 通过使用鼠标 1114 等在再现区域指定单元 32 中执行再现区域指定处理。可选择地, 也有可能自动地指定以前在 RAM115、HD 116 等中登记的所希望的区域。

[0076] 顺便说明, 作为待指定的区域的一个例子, 在该实施例中指定图像的空间区域。然而, 本发明不限于此。就是说, 显然可指定各种图像数据的部分区域。例如, 显然在 JPEG 2000 系统的图像数据中, 可指定预定分量, 并且可指定预定分辨率水平。

[0077] 随后,将解释重叠判断单元 33 的功能。就是说,重叠判断单元 33 通过把在输入(加密)图像数据中的加密区域与在以前阶段由再现区域指定单元 32 指定的再现区域 V 相比较,判断在加密区域与再现区域 V 之间是否有重叠。然后,重叠判断单元 33 根据判断结果控制切换单元 34。

[0078] 在该实施例中,如果判断再现区域 V 不重叠加密区域,则控制切换单元 34 连接到图像再现单元 38 上。同时,如果判断再现区域 V 重叠加密区域,则控制切换单元 34 连接到解密密钥获取单元 35 上。这里,应该注意,所述图像数据和解密相关信息被输出到连接的图像再现单元 38 或解密密钥获取单元 35。

[0079] 顺便说明,在该实施例中,如图 7 中所示,有可能通过分析在图像数据中的首部信息 82 的加密相关信息 84(就是说,图 7 的第一加密区域信息 Z1 和第二加密区域信息 Z2)知道加密区域。

[0080] 这里,将解释根据该实施例的解密相关信息。就是说,解密相关信息是包括在以后阶段对于在图像解密单元 37 中的图像解密处理必需的重叠区域信息、密钥信息及加密顺序信息的信息。在重叠判断单元 33 中,仅有来自重叠区域信息、密钥信息及加密顺序信息中的重叠区域信息被计算,并且记录在解密相关信息中。

[0081] 图 9A、9B 及 9C 用来解释可应用于实施例的解密相关信息。在重叠判断单元 33 中,仅记录在图 9A 中所示的重叠区域信息。这里,在图 9A 中,按如下通过使用第一加密区域信息 Z1、第二加密区域信息 Z2 及再现区域 V 计算第一重叠区域 VZ1 和第二重叠区域 VZ2。

$$VZ1 = Z1 \cap V \quad \dots (1)$$

$$VZ2 = Z2 \cap V \quad \dots (2)$$

[0084] 就是说,如公式 (1) 中所示第一重叠区域 VZ1 是第一加密区域信息 Z1 和再现区域 V 的交集,并且如公式 (2) 中所示第二重叠区域 VZ2 是第二加密区域信息 Z2 和再现区域 V 的交集。

[0085] 作为公式 (1) 的结果,如果第一重叠区域 VZ1 不是空集(就是说,如果打算再现加密区域),则计算的第一重叠区域 VZ1 与对应加密区域信息相关,并且记录在解密相关信息中,如图 9A 中所示。同样,作为公式 (2) 的结果,如果第二重叠区域 VZ2 不是空集(就是说,如果打算再现加密区域),则计算的第二重叠区域 VZ2 与对应加密区域信息相关,并且记录在解密相关信息中,如图 9A 中所示。

[0086] 这里,将参照图 10A、10B 及 10C 解释重叠区域的例子。就是说,图 10A 至 10C 用来解释根据实施例的重叠区域的例子。更明确地说,在图 10A 中,附图标记 141 指示第一加密区域(信息)Z1,附图标记 142 指示第二加密区域(信息)Z2,及附图标记 143 指示再现区域 V。除此之外,在图 10B 中的附图标记 144 指示第一重叠区域 VZ1,并且在图 10C 中的附图标记 145 指示第二重叠区域 VZ2。

[0087] 如图 10A 至 10C 中所示,通过使用公式 (1) 计算第一加密区域 141(Z1) 和再现区域 143(V) 的交集作为第一重叠区域 144(VZ1),并且通过使用公式 (2) 计算第二加密区域 142(Z2) 和再现区域 143(V) 的交集作为第二重叠区域 145(VZ2)。

[0088] 随后,将解释解密密钥获取单元 35 的功能。就是说,在解密密钥获取单元 35 中,图像数据和解密相关信息被首先输入,在以后阶段在图像解密单元中必需的密钥信息通过使用输入的解密相关信息获取,获取的密钥信息另外记录在解密相关信息中,获取的解密

相关信息然后与图像数据一起输出。

[0089] 这里,再次参照图 9A 至 9C 将解释如何获取密钥信息。就是说,在解密密钥获取单元 35 中,如图 9A 中所示的解密相关信息在以前阶段从重叠判断单元 33 输入。然后,在解密密钥获取单元 35 中,通过分析如图 7 中所示的首部信息(使用对应的加密区域信息)获取与每个重叠区域信息相对应的密钥信息。以后,如图 9B 中所示,获取的密钥信息与每个重叠区域信息相关,并且作为“密钥信息”被添加。

[0090] 在该实施例中,在其中密钥的标识符被记录(在首部信息中)作为密钥信息的情况下,通过请求密钥服务器 92 传输与相关标识符相对应的密钥信息来获取密钥信息。可选择地,如上所述,在其中通过使用第三密钥信息加密第一密钥信息和第二密钥信息的情况下,仅必须通过使用第三密钥信息解密每个被加密的密钥信息。

[0091] 如以上解释的那样,在解密密钥获取单元 35 中,获取与每个重叠区域相对应的密钥信息。

[0092] 以后,将解释加密顺序确定单元 36 的功能。就是说,在加密顺序确定单元 36 中,图像数据和解密相关信息被首先输入,然后确定按什么顺序相对于在解密相关信息中的重叠区域执行加密处理,所确定的加密顺序信息额外记录在解密相关信息中,及获取的解密相关信息与图像数据一起输出。

[0093] 这里,再次参照图 9A 至 9C 将解释如何确定加密顺序。就是说,在加密顺序确定单元 36 中,如图 9B 中所示的解密相关信息在以前阶段从解密密钥获取单元 35 输入。然后,在加密顺序确定单元 36 中,通过分析如图 7 中所示的首部信息(使用对应的加密区域信息),确定按什么顺序加密相应重叠区域。以后,如图 9C 中所示,确定的图像加密顺序与各个重叠区域相关,并且额外记录为加密顺序信息。

[0094] 如以上解释的那样,相应重叠区域的加密顺序在加密顺序确定单元 36 中确定。顺便说明,在该实施例中,有可能把如图 9C 中所示的解密相关信息在以后阶段按原样输出到图像解密单元 37。然而,由于加密区域信息在图像解密单元 37 中是不需要的,所以也有可能擦除加密区域信息。

[0095] 以后,将解释图像解密单元 37 的功能。就是说,在图像解密单元 37 中,图像数据和解密相关信息被首先输入,通过使用解密相关信息对于输入图像数据执行图像解密处理,然后输出获取的图像数据。

[0096] 以后将描述在该实施例中的图像解密处理的细节。

[0097] 这样,在图像再现单元 38 中,来自切换单元 34 或图像解密单元的输出最后输出到监视器 112。除此之外,输出图像数据可存储在 RAM 115、HD 116、CD-ROM 驱动器 117、FD 驱动器 118 及 DVD-ROM 驱动器 119 中。另外,输出图像数据也可由 NIC 1110 通过因特网传输到另一个计算机。

[0098] 如上所述,解释了可应用于该实施例的图像再现处理和执行图像再现处理的方法。

[0099] 以后,参照图 11 将解释以上图像再现处理的流程。就是说,图 11 是流程图,用来解释可应用于该实施例的图像再现处理。

[0100] 最初,希望的图像区域首先在步骤 S41 中指定,并且在步骤 S42 和 S43 中判断在再现区域与加密区域之间的重叠。然后,如果判断有重叠,则流程前进到步骤 S44,而如果判断

没有重叠，则流程前进到步骤 S47。顺便说明，与重叠区域相对应的解密密钥在步骤 S44 中获取，然后加密的自适应顺序在步骤 S45 中确定。以后，图像解密处理在步骤 S46 中执行，并且最后在步骤 S47 中再现图像。

[0101] 图 12 是方块图，用来解释根据实施例的图像解密处理功能和实现图像解密处理功能的方法。更明确地说，图 12 表示在图 8 中表示的图像解密单元 37 的构造。在该图中，附图标记 51 指示加密区域确定单元，并且附图标记 52 指示切换单元。

[0102] 最初，将解释加密区域确定单元 51 的功能。就是说，在加密区域确定单元 51 中，输入图像数据和解密相关信息（如图 9 中所示），并且然后通过使用解密相关信息而输出待经受解密处理的重叠区域信息、对应密钥信息、及图像数据。

[0103] 这里，在加密区域确定单元 51 中，输出从与在解密相关信息中具有加密顺序信息的最大值的记录相对应的重叠区域信息、和密钥信息开始。这是因为加密顺序信息较大的重叠区域是在加密步骤中较晚加密的区域。就是说，在该实施例中控制较晚加密的区域较早经受解密处理。

[0104] 随后，将解释解密单元 52 的功能。就是说，在解密单元 52 中，重叠区域信息和对应密钥信息与图像数据一起输入，由图像数据中的重叠区域指示的区域通过使用密钥信息经受解密处理，然后所获取的图像数据被输出。

[0105] 在解密单元 52 中，执行与在图 4 中表示的加密单元 14 中待执行的处理相对应的解密处理。顺便说明，应该注意，擦除在解密相关信息中包括的与经受解密处理的重叠区域相对应的记录（以便指示已经执行解密处理）。

[0106] 接下来，将解释切换单元 53 的功能。就是说，切换单元 53 判断在通过解密单元 52 的解密处理被执行之后是否剩下待经受解密处理的重叠区域。然后，如果在解密相关信息中记录仍然剩下，则切换单元 53 连接到加密区域确定单元 51 上。同时，如果记录没有剩下，则切换单元 53 连接到以上图像再现单元 38 上。

[0107] 随后，参照图 13 将描述以上图像解密处理的流程。这里，图 13 是流程图，表示可应用于实施例的图像解密处理。

[0108] 最初，在步骤 S61 中，确定将经受解密处理的加密区域。接下来，在步骤 S62 中，对于确定的加密区域执行解密处理。在解密处理被执行之后，在步骤 S63 中判断整个解密处理是否结束。然后，如果判断整个解密处理未结束，则流程返回到步骤 S61。同时，如果判断整个解密处理结束，则图像解密处理结束。

[0109] 这里，参照图 14A、14B、14C、14D 及 14E 将解释由该实施例能够实现的图像再现的例子。

[0110] 就是说，图 14A 至 14E 用来解释由该实施例能够实现的图像再现的例子。更明确地说，图 14A 表示未加密并因而待加密的图像数据。另外，图 14B 表示其中在对于第一加密区域 71 执行第一加密处理之后对于第二加密区域 72 执行第二加密处理的图像数据。这里，在图 14B 中的附图标记 73 指示第一加密区域 71 和第二加密区域 72 的交集。

[0111] 图 14C 解释其中第一重叠区域 VZ1 和第二重叠区域 VZ2 是空集的情形。这里，在图 14C 中的附图标记 74 在这种情况下指示再现区域 V。当再现区域 V 由再现区域指定单元 32 指定时，由重叠判断单元 33 判断再现区域 V74 不重叠第一加密区域 71 和第二加密区域 72。因而，未执行任何解密处理，并且再现区域 V74 由图像再现单元 38 再现。

[0112] 图 14D 解释其中重叠区域 VZ1 不是空集的情形（就是说，第二重叠区域 VZ2 是空集）。这里，在图 14D 中的附图标记 75 在这种情况下指示再现区域 V。当再现区域 V75 由再现区域指定单元 32 指定时，由重叠判断单元 33 判断再现区域 V75 仅重叠第一加密区域 71。结果，第一加密区域 71 和再现区域 V75 的交集被确定为第一重叠区域 VZ1。而且，与第一加密区域 71 相对应的第一密钥信息 K1 在解密密钥获取单元 35 中获取。此后，与第一加密处理相对应的解密处理在图像解密单元 37 中通过使用第一密钥信息 K1 而执行，并且再现区域 V75 在图像再现单元 38 中再现。

[0113] 图 14E 解释其中第一重叠区域 VZ1 和第二重叠区域 VZ2 都不是空集的情形。这里，在图 14E 中的附图标记 76 在这种情况下指示再现区域 V。当再现区域 V76 由再现区域指定单元 32 指定时，由重叠判断单元 33 判断再现区域 V76 与第一加密区域 71 和第二加密区域 72 都重叠。结果，第一加密区域 71 和再现区域 V76 的交集被确定为第一重叠区域 VZ1，并且第二加密区域 72 和再现区域 V76 的交集被确定为第二重叠区域 VZ2。而且，在解密密钥获取单元 35 中，获取与第一加密区域 71 相对应的第一密钥信息 K1，并且获取与第二加密区域 72 相对应的第二密钥信息 K2。随后，在加密顺序确定单元 36 中，判断在已经加密第一重叠区域之后加密第二重叠区域，并且在图像解密单元 37 中执行预定解密处理。最后，在图像再现单元 38 中使再现区域 V76 再现。

[0114] 顺便说明，在以上解释中加密执行两次。然而，不用说，本发明也可应用于其中加密执行三次或更多次的情形。例如，如果第一重叠区域和第三重叠区域是空集并且第二重叠区域不是空集，则与第一加密区域相对应的第一密钥信息和与第三加密区域相对应的第三密钥信息分别在解密密钥获取单元 35 中获取。随后，由加密顺序确定单元 36 确定在已经加密第一重叠区域之后加密了第三重叠区域，并且在图像解密单元 37 中执行解密第三加密和解密第一加密的处理。

[0115] 顺便说明，在该实施例中，作为在图 8 中表示的再现区域指定单元 32 的功能，举例解释指定所希望的再现区域的功能。然而，本发明不限于此。就是说，也有可能作为再现区域指定单元 32 指定所希望的解密区域的功能。在该情况下，预先扰码的图像数据显示在图 2 中表示的图像查看器中。然后，在再现区域指定单元 32 中，就是说，通过使用矩形 106、用于分辨率水平的空白栏 1010、用于层的空白栏 1011、及用于分量的空白栏 1012，仅需适当地指定待经受解密处理的图像区域。

[0116] 在任何情况下，如以上那样解释了根据本发明的实施例。这里，如以前解释的那样，加密图像数据和解密加密的图像数据的装置是诸如普通个人计算机之类的通用信息处理装置，并且以上功能可由在个人计算机上运行的计算机程序实现。为此，显然本发明的概念包括计算机程序。此外，典型地，计算机程序存储在诸如 CD-ROM 等之类的计算机可读存储介质中。那么，通过把计算机可读存储介质设置到计算机的对应驱动器和安装在设置存储介质中存储的程序，可执行相关计算机程序。为此，也显然的是，本发明的概念包括计算机可读存储介质本身。

[0117] 根据该实施例，当部分加密和多重加密图像数据经受局部解密时，有可能确定相关区域的哪一个已经经受多重加密，借此有可能防止不必要地获取对于解密是多余的密钥。此外，有可能相对于待解密和再现的区域确定解密顺序，有可能防止全部解密经受多重加密的区域。因而，在安全性方面是安全的，并且有可能防止无用解密。

[0118] 根据本发明,有可能适当地执行图像数据的局部解密,其中所述图像数据已经执行局部加密和 / 或多重加密。

[0119] 换句话说,实施例的以上描述仅为了说明目的而给出,并且不要理解成在各个方面施加任何限制。

[0120] 本发明的范围因此仅由如下权利要求书确定,并且不由说明书的正文限制,及在等效于附属权利要求书范围的范围内进行的变更落在本发明的真实精神和范围内。

[0121] 本申请要求来自于 2004 年 9 月 7 日提交的日本专利申请 No. 2004-259633 的优先权,该专利申请由此通过参考包括在这里。

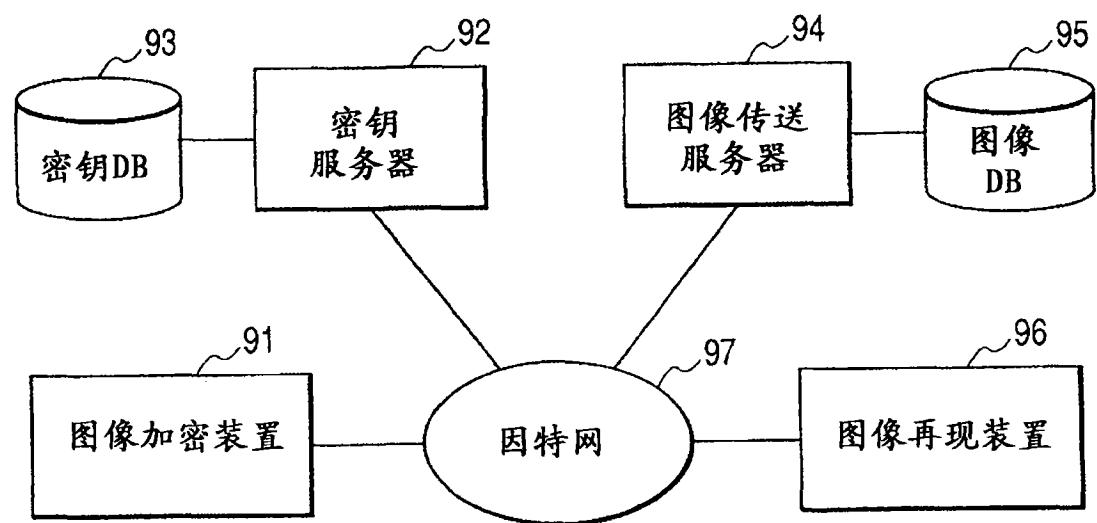


图 1

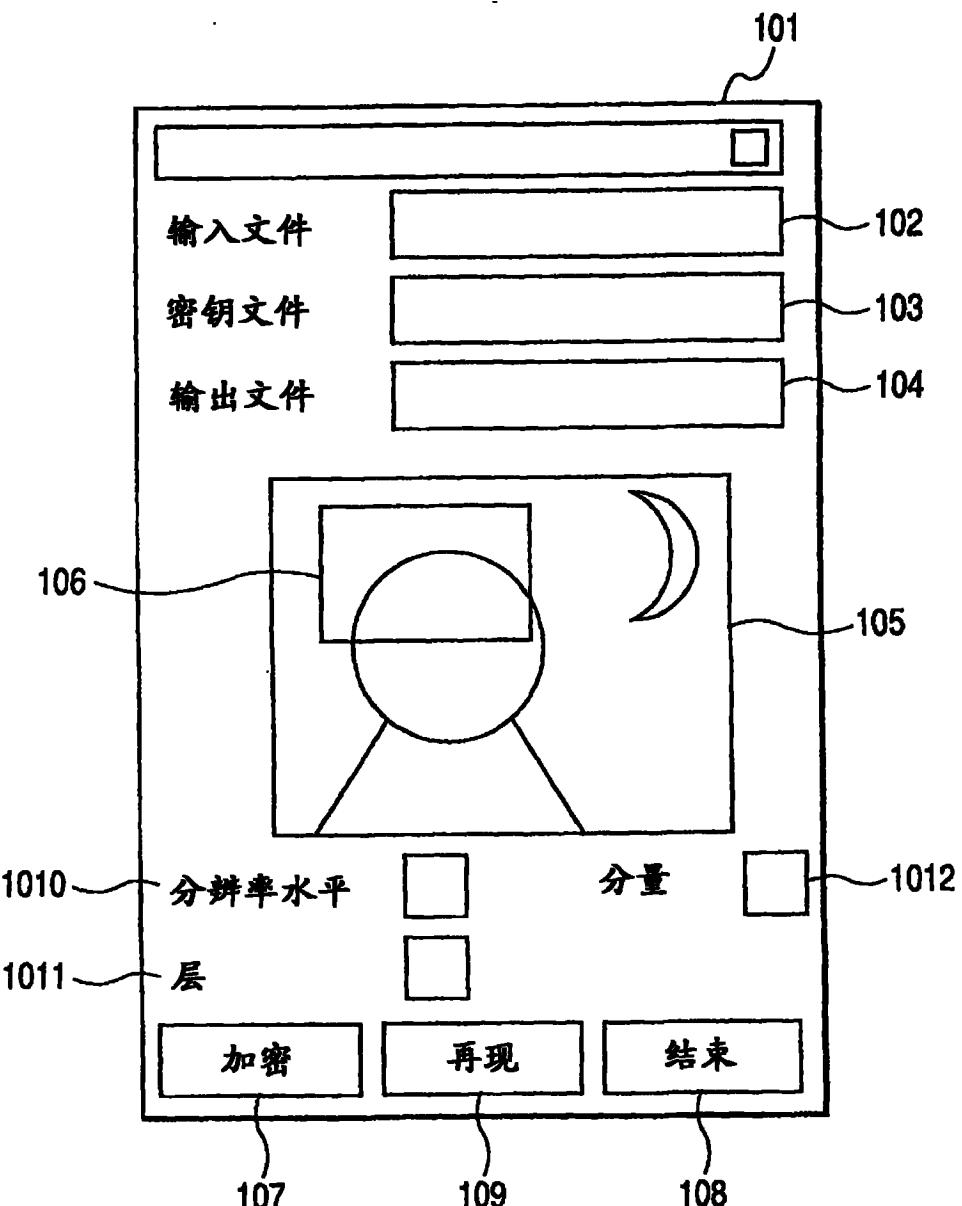


图 2

图 3

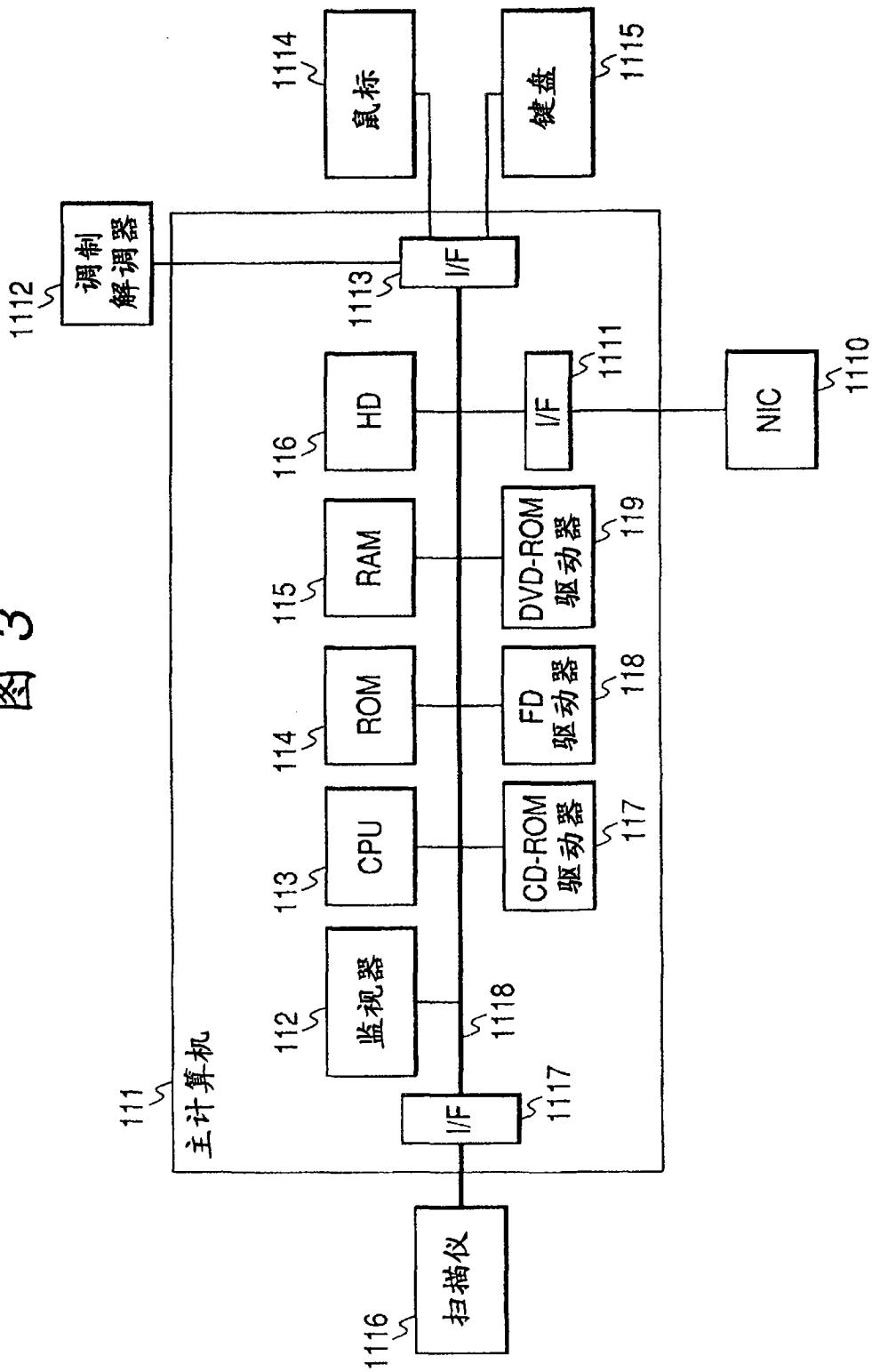


图 4

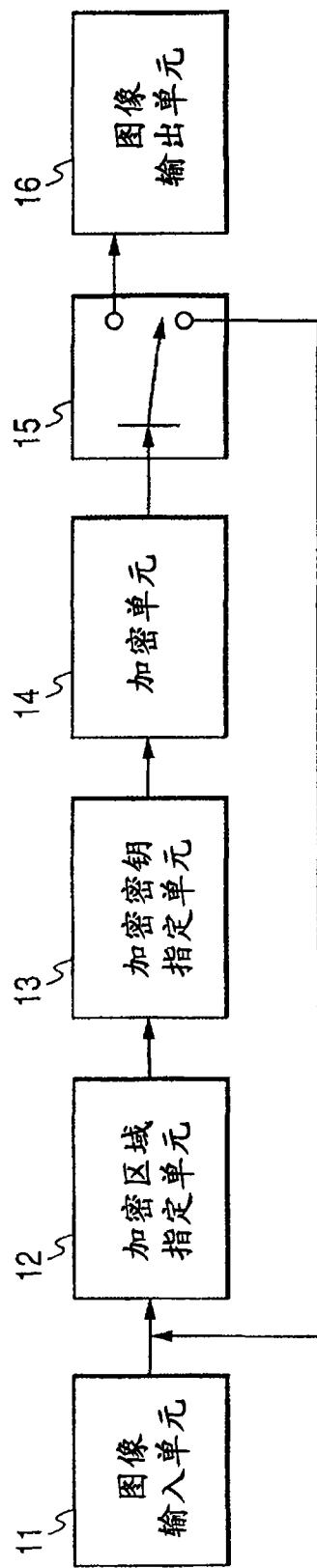


图 5A

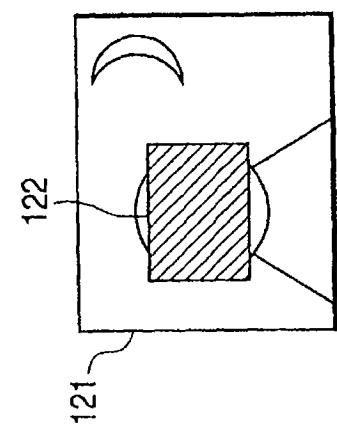


图 5B

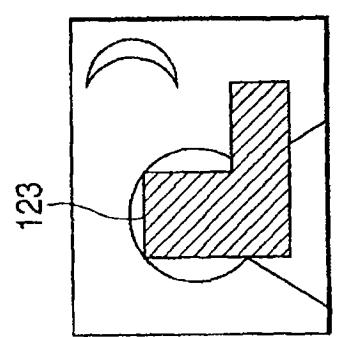
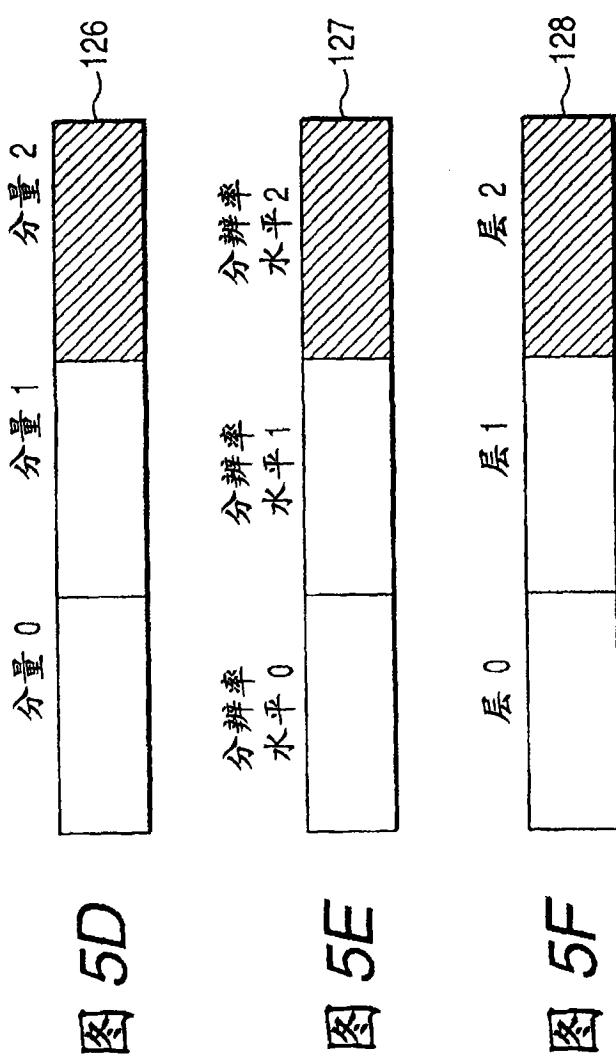
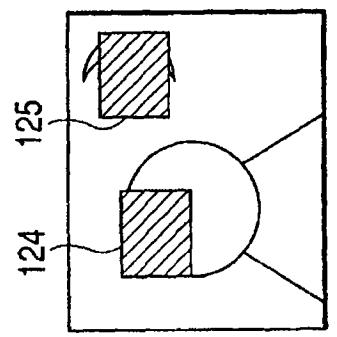


图 5C



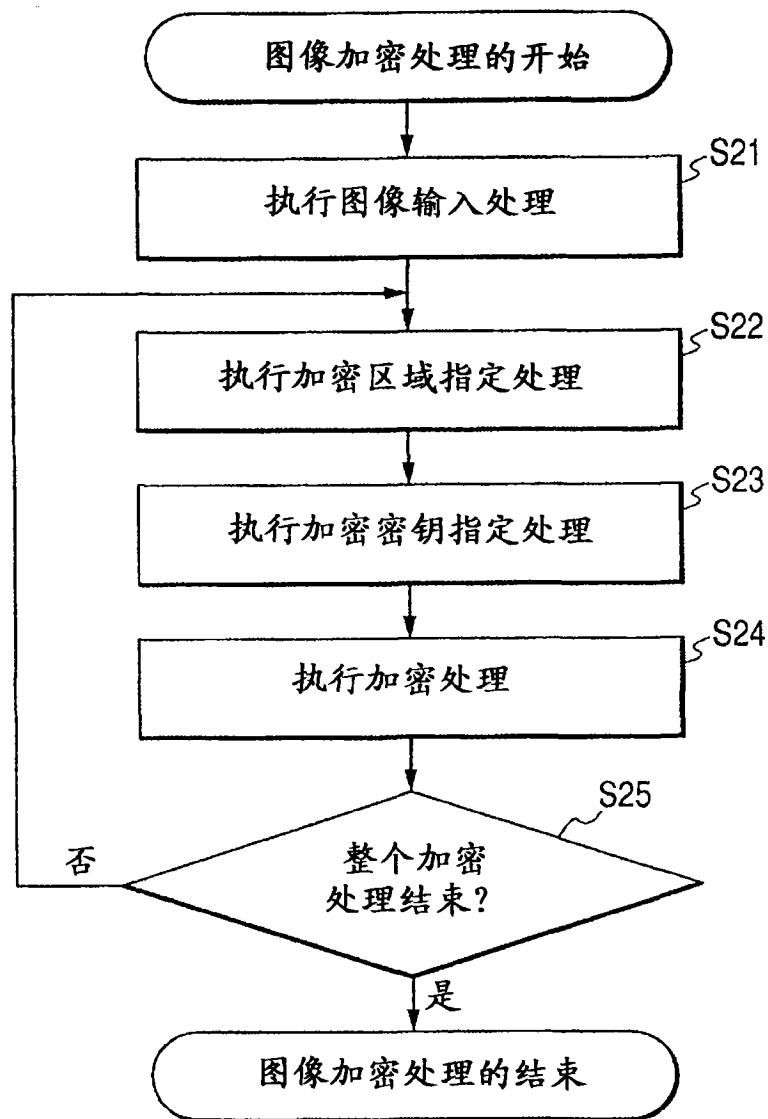


图 6

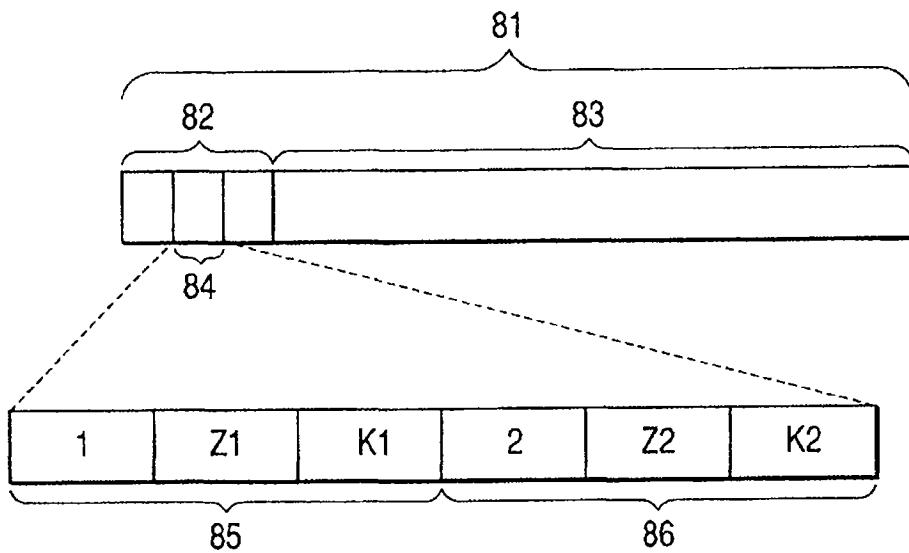
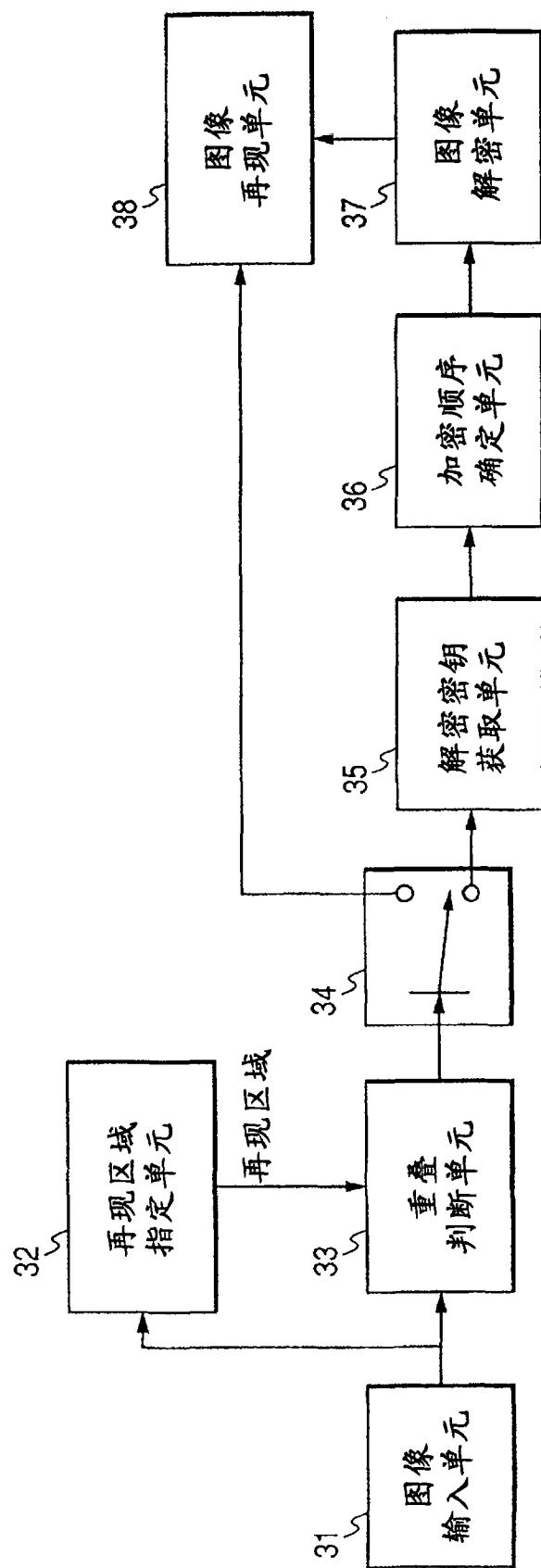


图 7

图 8



加密 区域信息	重叠 区域信息
Z1	VZ1
Z2	VZ2

图 9A

加密 区域信息	重叠 区域信息	密钥信息
Z1	VZ1	K1
Z2	VZ2	K2

图 9B

加密 区域信息	重叠 区域信息	密钥信息	加密 顺序信息
Z1	VZ1	K1	1
Z2	VZ2	K2	2

图 9C

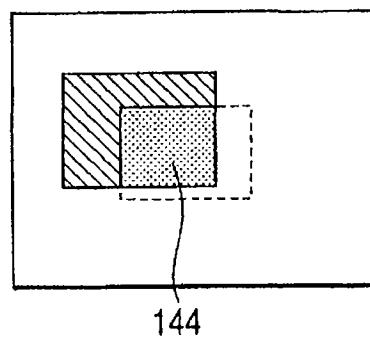
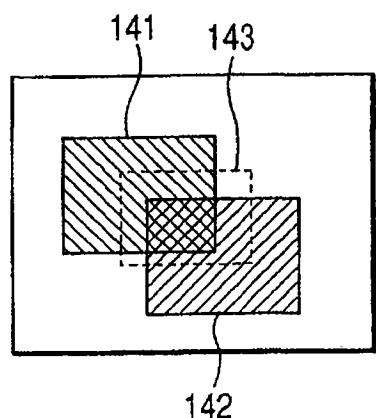


图 10B

图 10A

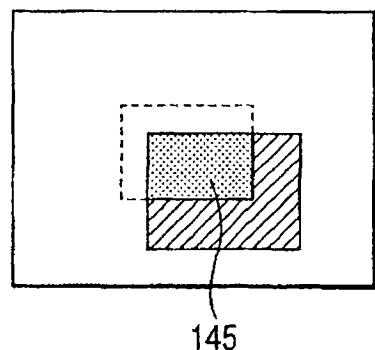


图 10C

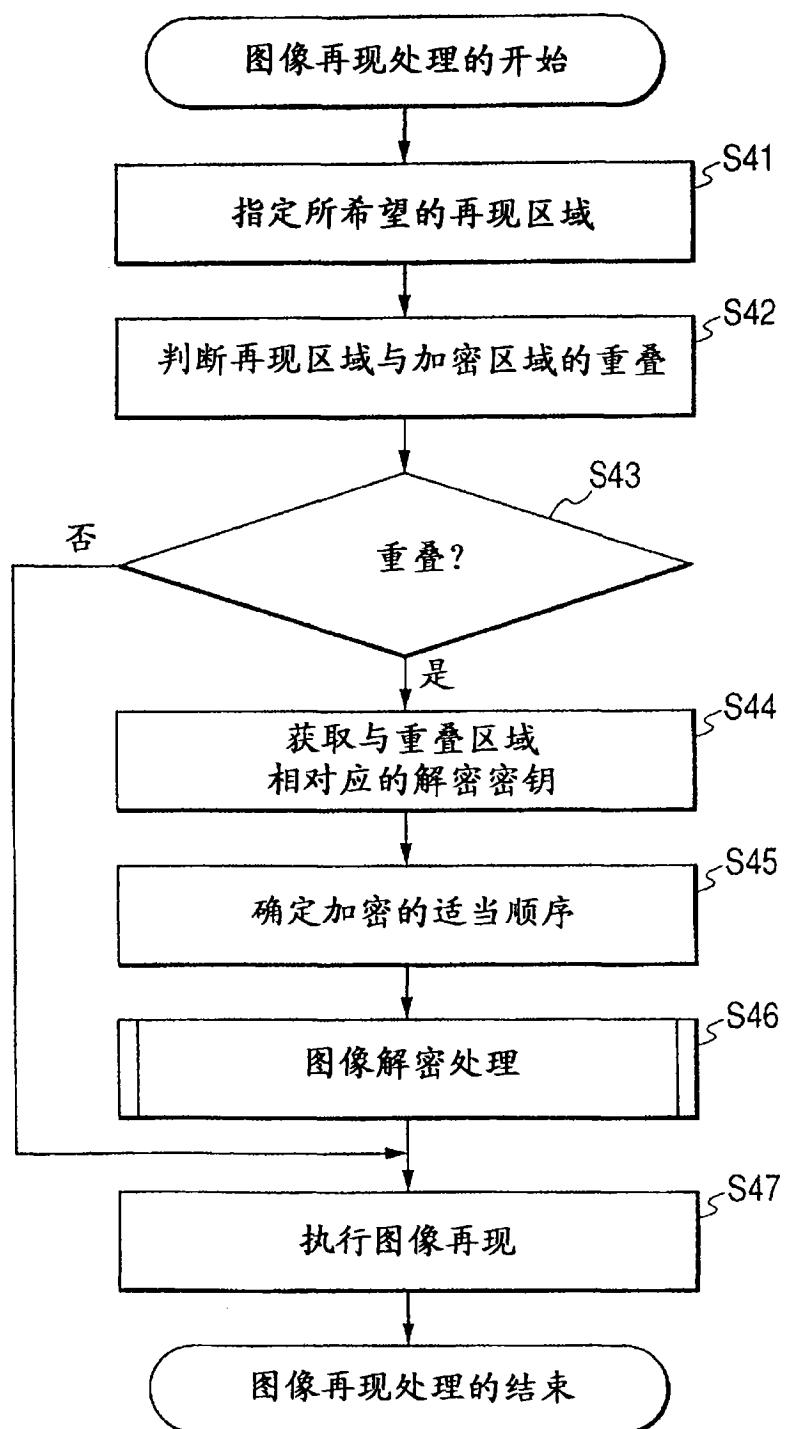


图 11

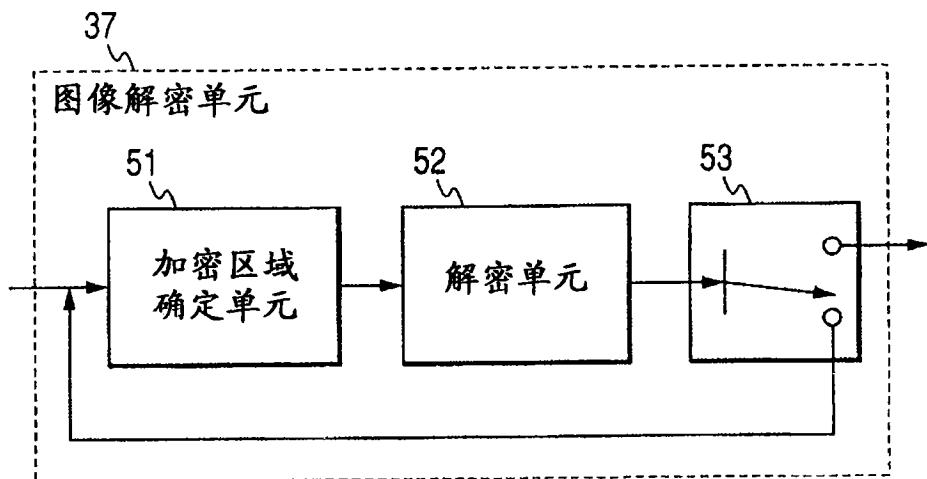


图 12

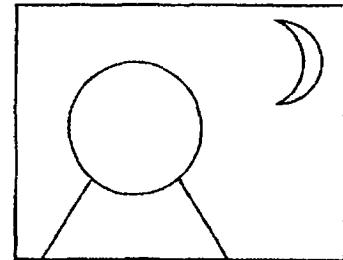
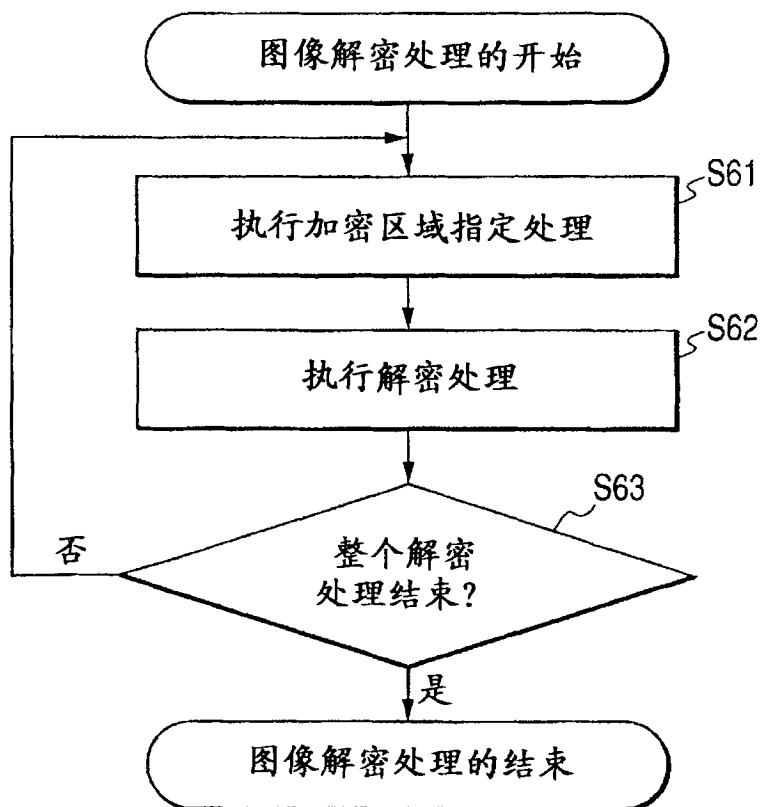


图 14A

图 13

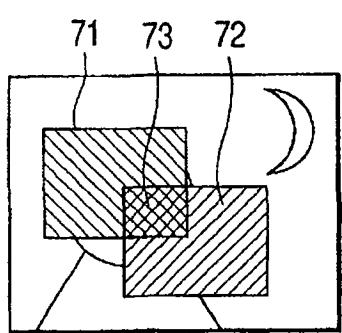


图 14B

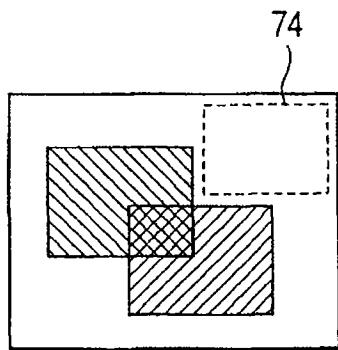


图 14C

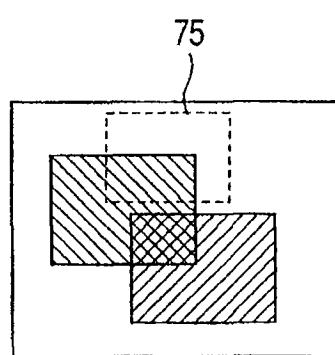


图 14D

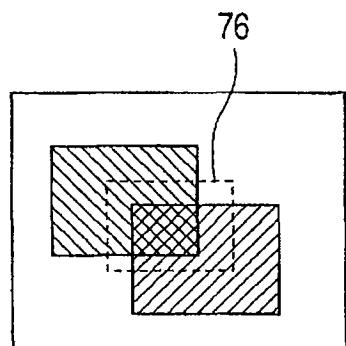


图 14E