(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105243309 A
(43)申请公布日 2016.01.13

(21)申请号 201510645660.X

(22)申请日 2015.10.08

(71)申请人 宁波大学
地址 315211 浙江省宁波市江北区风华路818号

(72)发明人 郑紫微 丁石磊

(74)专利代理机构 宁波诚源专利事务所有限公司 33102
代理人 刘凤钦

(51)Int.Cl.
G06F 21/32(2013.01)
G06F 21/60(2013.01)

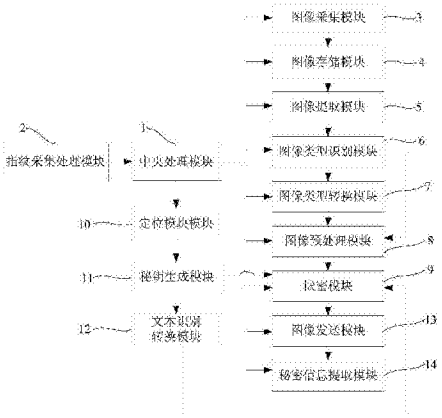
权利要求书4页 说明书9页 附图3页

(54)发明名称

基于智能移动终端图像的工业图纸加密系统及其加密方法

(57)摘要

本发明涉及基于智能移动终端图像的工业图纸加密系统及其加密方法，智能移动终端包括中央处理模块及分别连接中央处理模块的指纹采集处理模块、图像采集模块、图像存储模块、图像提取模块、图像类型识别模块、图像类型转换模块、图像预处理模块、嵌密模块、定位模块、秘钥生成模块、文本识别转换模块、图像发送模块和秘密信息提取模块；图像存储模块连接图像采集模块和图像提取模块，图像预处理模块连接图像类型识别模块、图像类型转换模块和嵌密模块，定位模块连接秘钥生成模块，文本识别转换模块连接嵌密模块，图像发送模块连接嵌密模块、秘钥生成模块和秘密信息提取模块，既能识别移动终端操作者合法身份，又能将秘密信息安全嵌入到工业图纸中。



CN 105243309 A

1. 基于智能移动终端图像的工业图纸加密系统，其特征在于，所述智能移动终端包括中央处理模块以及分别连接中央处理模块的指纹采集处理模块、图像采集模块、图像存储模块、图像提取模块、图像类型识别模块、图像类型转换模块、图像预处理模块、嵌密模块、定位模块、秘钥生成模块、文本识别转换模块、图像发送模块和秘密信息提取模块；所述图像存储模块分别连接图像采集模块和图像提取模块，所述图像预处理模块分别连接图像类型识别模块、图像类型转换模块和嵌密模块，所述定位模块连接秘钥生成模块，所述文本识别转换模块连接嵌密模块，所述图像发送模块分别与嵌密模块、秘钥生成模块和秘密信息提取模块连接，其中，

所述中央处理模块，根据指纹采集处理模块采集到的智能移动终端操作者的指纹信息，并判断与预设智能移动终端的合法拥有者指纹信息一致时，则命令移动终端开放嵌入秘密信息的权限给移动终端的操作者，并命令连接中央处理模块的各模块启动；

所述指纹采集处理模块，用以采集智能移动终端操作者的指纹信息，并发送采集到的智能移动终端操作者的指纹信息给中央处理模块；

所述图像采集模块，用以采集工业图纸为外部图像，并对采集的外部图像自动编号，存储至图像存储模块；

所述图像存储模块，一方面保存图像采集模块编号的外部图像，一方面保存系统预先存储的图像；

所述图像提取模块，用于提取图像存储模块中的图像，并发送给图像类型识别模块；

所述图像类型识别模块，用以判断所接收的图像类型为动态图像时，则将其发送给图像预处理模块处理；判断接收的图像为静态图像时，则发送图像给图像类型转换模块处理；

所述图像类型转换模块，用以将接收的静态图像转换为动态图像，并发送转换后的动态图像给图像预处理模块；

所述图像预处理模块，用以对接收的动态图像进行滤噪或加噪处理，并将滤噪或加噪后的动态图像分解成多个不同帧长的帧图像，并将各帧图像分别作为载体图像发送给嵌密模块嵌入秘密信息；

所述嵌密模块，用以将字符串形式的秘密信息嵌入到接收的滤噪或加噪后的载体图像中，并将载密图像发送给图像发送模块；

所述定位模块，用以获取移动终端当前所处的位置数据，并发送获取的位置数据给秘钥生成模块；

所述秘钥生成模块，接收位置数据，并以接收的位置数据作为与载密图像对应的加密秘钥，并将生成的加密秘钥发送给图像发送模块；

所述文本识别转换模块，用于识别需要加密的信息为非字符串形式时，将非字符串形式的信息转换为字符串形式的加密信息，并发送给嵌密模块；识别需要加密的信息为字符串形式的信息时，则直接发送给嵌密模块；

所述图像发送模块，将接收的加密秘钥、载密图像以及其他帧图像一起保存到图像存储模块；所述秘密信息提取模块，用以利用对应加密秘钥的解密秘钥提取载密图像中的秘密信息。

2. 一种权利要求 1 所述工业图纸加密系统的加密方法，其特征在于，依次包括如下步

骤：

(1) 指纹采集处理模块采集智能移动终端操作者的指纹信息给中央处理模块，中央处理模块判断采集的指纹信息与预设的智能移动终端合法拥有者的指纹信息一致时，则命令图像采集模块采集外部图像后进行自动编号，并保存至图像存储模块中；

(2) 图像提取模块提取图像存储模块中存储的外部图像或系统预存图像，并将提取的图像发送给图像类型识别模块进行识别；

(3) 图像类型识别模块判断图像类型为动态图像时，则将其发送给图像预处理模块；判断接收的图像为静态图像时，则发送图像给图像类型转换模块，由图像类型转换模块将静态图像转换为动态图像，并发送给图像预处理模块；

(4) 文本识别转换模块识别需要加密的信息为非字符串形式时，将非字符串形式的信息转换为字符串形式的加密信息，并发送给嵌密模块；识别需要加密的信息为字符串形式的信息时，则直接发送给嵌密模块；

(5) 图像预处理模块对接收的动态图像进行滤噪或加噪处理，将滤噪或加噪后的动态图像以预设的时间段分解成多个不同帧长的帧图像，并将各帧图像分别作为待选载体图像发送给嵌密模块嵌入秘密信息；其中，嵌密模块嵌入秘密信息的过程依次包括如下步骤：

(5-1) 在多个载体图像中选择其中一个图像作为目标载体图像C，设目标载体图像C的像素值为c×c，设定待嵌入的秘密信息S为一组长度为L的字符串s，记字符串s中第i个字符为s_i，$1 \leqslant i \leqslant L$；

(5-2) 统计字符串s中各字符出现的次数，并计算出各字符的出现概率，记字符s_i的出现概率为$p(s_i)$，$0<p(s_i) \leqslant 1$；

(5-3) 根据各字符出现概率从小到大的顺序，对各字符进行重新排序，形成一组新的字符串s_1，并查找新的字符串s_1中出现概率最小的字符；

(5-4) 以新字符串中字符从左至右的顺序查找，将查找到的出现概率最小的字符组合相加，形成新的节点，并将形成的新节点作为整体与其他未组合的字符重新排序；

(5-5) 再次重复执行步骤(5-4)，以最终得到概率之和为1，获得最终的Huffman二叉树；根据Huffman二叉树，以从根到分支、左节点为0，右节点为1的原则，得到Huffman码表；

(5-6) 根据Huffman码表中各字符对应的编码顺序，得到待嵌入秘密信息S的编码信息数据D，其中设定编码信息数据D的长度为l，第j个信息数据为d_j，$1 \leqslant j \leqslant l$；

(5-7) 以IP置换表，对步骤(5-6)中编码信息数据D进行重新排序，以获得置换编码信息数据D_0，其中，置换编码信息数据D_0由位于左侧的L_0数据组和位于右侧的R_0数据组组成，$D_0 = L_0R_0$，该重新排序过程包括如下步骤(a)至步骤(f)：

(a) 将编码信息数据D中第58位信息数据d_{58}作为L_0数据组的第1位，编码信息数据D中第50位信息数据d_{50}作为L_0数据组中的第2位，依此类推，得到L_0数据组为$L_0 = d_{58}d_{50}d_{42}\cdots d_8$；编码信息数据D中第57位信息数据$d_{57}$作为$R_0$数据组的第1位，编码信息数据D中第49位信息数据$d_{49}$作为$L_0$数据组中的第2位，依此类推，得到$R_0$数据组为$R_0 = d_{57}d_{49}d_{41}\cdots d_7$；将$L_0$数据组和$R_0$数据组进行组合，得到置换编码信息数据$D_1 = d_{58}d_{50}d_{42}\cdots d_8d_{57}d_{49}d_{41}\cdots d_7$；

(b) 对步骤(b)所得L_0数据组和R_0数据组中数据按照IP置换表进行IP置换和异或

运算，并进行 16 次循环迭代，得到迭代后的 L'_0 数据组和 R'_0 数据组，并令 $L'_0(t) = L_0(t)$，$R'_0 = R_0(t)$，其中，迭代公式如下：

$$L_0(t) = R_0(t-1);\quad R_0(t) = L_0(t) \oplus f\left(R_0(t-1), k_t\right),\quad t = 1,2,\cdots,16;$$

其中，$L_0(t)$ 表示 L_0 数据组中第 t 个信息数据，$R_0(t)$ 表示 R_0 数据组中第 t 个信息数据，⊕表示异或运算，f(,) 表示由 S 盒决定的置换算法，k_t 表示由密钥编排产生的数据块；

IP 置换表如下：

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	3	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

(c) 对步骤 (b) 所得迭代后的 L'_0 数据组和 R'_0 数据组中的数据按照 IP^{-1} 逆置换表进行置换，得到密文数据 D'；其中，IP^{-1} 逆置换表如下：

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

(d) 将预处理后的秘密信息中每个比特按 zigzag 扫描的方式对应于载体图像 C 的各个像素值，并记录像素的 LSB 数据流；

(e) 统计每个像素的 LSB 与欲嵌入的秘密信息比特不同的像素个数，记不同的像素构成向量 g，并计算、获取最优组合 $x_0, x_1, x_2, \cdots, x_{255}$；其中，最优组合 $x_0, x_1, x_2, \cdots, x_{255}$ 的求解公式如下：

$$\sum_{j=2i} x_j + \sum_{j=2i+1} (g_j - x_j) = \sum_{j=2i} (g_j - x_j) + \sum_{j=2i+1} x_j$$

$g' = Mx + g_s$，g' 表示图像隐写后的像素矩阵；

$$x_t = \begin{cases} 0, x_t < 0 \\ g_t, x_t > g_t \\ \lfloor x_t \rfloor, 0 \le x_t \le g_t \end{cases},\quad t = 1,2,\cdots,255;$$

$$d = \left\| \mathbf{g}' - \mathbf{g} \right\| = \sqrt{\sum_{j=0}^{255} \left(g'_j - g_j \right)^2};$$

(f) 对于灰度值为 g_j 的像素点集合 $(g_0, g_1, g_2, \cdots, g_{255})$，选择 x_j 个像素将其灰度值减 1，并将剩余的 $(g_j - x_j)$ 个像素的灰度值加 1，从而得到嵌入秘密信息 S 的加密载体图像 C'，其中，加密载体图像 C' 的像素矩阵为 g'；

(6) 定位模块获取移动终端当前所处的位置数据，并发送获取的位置数据给秘钥生成

模块；

(7) 秘钥生成模块接收位置数据，以接收的位置数据作为与载密图像对应的加密秘钥，并将生成的加密秘钥发送给图像发送模块；

(8) 图像发送模块将接收的加密秘钥、载密图像以及其他帧图像一起保存到图像存储模块，秘密信息提取模块则根据预先已知的解密秘钥提取载密图像中的秘密信息。

基于智能移动终端图像的工业图纸加密系统及其加密方法

技术领域

[0001] 本发明涉及移动终端保密领域，尤其涉及一种基于智能移动终端图像的工业图纸加密系统及其加密方法。

背景技术

[0002] 随着智能移动终端的日益普及，使用智能移动终端的移动互联网的用户占据越来越大的比重。移动互联网的飞速发展使得智能移动终端中图像、视频等数字多媒体信息的存储、复制与传播变得非常方便。利用智能移动终端处理工业图纸成为制造业领域的新趋势。在制造业领域中，工业图纸中的技术参数属于企业的技术秘密，一旦技术参数因工业图纸的泄漏而遭到公开，将会给企业生产带来极大的损失。

[0003] 然而，当人们为了方便，使用智能移动终端处理工业图纸，例如，对工业图纸的技术参数加密时，现有的技术参数加密方法不仅不能有效地识别移动终端操作者的合法身份，而且在工业图纸中加密后的技术参数非常容易被破解、提取，从而不利于技术参数的保护。

发明内容

[0004] 本发明所要解决的首要技术问题是针对上述现有技术提供一种既能识别移动终端操作者的合法身份，又能安全地将技术参数嵌入到工业图纸中的基于智能移动终端图像的工业图纸加密系统。

[0005] 本发明所要解决的进一步技术问题是提供一种上述工业图纸加密系统的加密方法。

[0006] 本发明解决上述首要技术问题所采用的技术方案为：基于智能移动终端图像的工业图纸加密系统，其特征在于，所述智能移动终端包括中央处理模块以及分别连接中央处理模块的指纹采集处理模块、图像采集模块、图像存储模块、图像提取模块、图像类型识别模块、图像类型转换模块、图像预处理模块、嵌密模块、定位模块、秘钥生成模块、文本识别转换模块、图像发送模块和秘密信息提取模块；所述图像存储模块分别连接图像采集模块和图像提取模块，所述图像预处理模块分别连接图像类型识别模块、图像类型转换模块和嵌密模块，所述定位模块连接秘钥生成模块，所述文本识别转换模块连接嵌密模块，所述图像发送模块分别与嵌密模块、秘钥生成模块和秘密信息提取模块连接，其中，

[0007] 所述中央处理模块，根据指纹采集处理模块采集到的智能移动终端操作者的指纹信息，并判断与预设智能移动终端的合法拥有者指纹信息一致时，则命令移动终端开放嵌入秘密信息的权限给移动终端的操作者，并命令连接中央处理模块的各模块启动；

[0008] 所述指纹采集处理模块，用以采集智能移动终端操作者的指纹信息，并发送采集到的智能移动终端操作者的指纹信息给中央处理模块；

[0009] 所述图像采集模块，用以采集工业图纸为外部图像，并对采集的外部图像自动编号，存储至图像存储模块；

[0010] 所述图像存储模块，一方面保存图像采集模块编号的外部图像，一方面保存系统预先存储的图像；

[0011] 所述图像提取模块，用于提取图像存储模块中的图像，并发送给图像类型识别模块；

[0012] 所述图像类型识别模块，用以判断所接收的图像类型为动态图像时，则将其发送给图像预处理模块处理；判断接收的图像为静态图像时，则发送图像给图像类型转换模块处理；

[0013] 所述图像类型转换模块，用以将接收的静态图像转换为动态图像，并发送转换后的动态图像给图像预处理模块；

[0014] 所述图像预处理模块，用以对接收的动态图像进行滤噪或加噪处理，并将滤噪或加噪后的动态图像分解成多个不同帧长的帧图像，并将各帧图像分别作为载体图像发送给嵌密模块嵌入秘密信息；

[0015] 所述嵌密模块，用以将字符串形式的秘密信息嵌入到接收的滤噪或加噪后的载体图像中，并将载密图像发送给图像发送模块；

[0016] 所述定位模块，用以获取移动终端当前所处的位置数据，并发送获取的位置数据给秘钥生成模块；

[0017] 所述秘钥生成模块，接收位置数据，并以接收的位置数据作为与载密图像对应的加密秘钥，并将生成的加密秘钥发送给图像发送模块；

[0018] 所述文本识别转换模块，用于识别需要加密的信息为非字符串形式时，将非字符串形式的信息转换为字符串形式的加密信息，并发送给嵌密模块；识别需要加密的信息为字符串形式的信息时，则直接发送给嵌密模块；

[0019] 所述图像发送模块，将接收的加密秘钥、载密图像以及其他帧图像一起保存到图像存储模块；所述秘密信息提取模块，用以利用对应加密秘钥的解密秘钥提取载密图像中的秘密信息。

[0020] 进一步地，智能移动终端图像的工业图纸加密方法，其特征在于，依次包括如下步骤：

[0021] (1) 指纹采集处理模块采集智能移动终端操作者的指纹信息给中央处理模块，中央处理模块判断采集的指纹信息与预设的智能移动终端合法拥有者的指纹信息一致时，则命令图像采集模块采集外部图像后进行自动编号，并保存至图像存储模块中；

[0022] (2) 图像提取模块提取图像存储模块中存储的外部图像或系统预存图像，并将提取的图像发送给图像类型识别模块进行识别；

[0023] (3) 图像类型识别模块判断图像类型为动态图像时，则将其发送给图像预处理模块；判断接收的图像为静态图像时，则发送图像给图像类型转换模块，由图像类型转换模块将静态图像转换为动态图像，并发送给图像预处理模块；

[0024] (4) 文本识别转换模块识别需要加密的信息为非字符串形式时，将非字符串形式的信息转换为字符串形式的加密信息，并发送给嵌密模块；识别需要加密的信息为字符串形式的信息时，则直接发送给嵌密模块；

[0025] (5) 图像预处理模块对接收的动态图像进行滤噪或加噪处理，将滤噪或加噪后的动态图像以预设的时间段分解成多个不同帧长的帧图像，并将各帧图像分别作为待选载体

图像发送给嵌密模块嵌入秘密信息；其中，嵌密模块嵌入秘密信息的过程依次包括如下步骤：

[0026] (5-1) 在多个载体图像中选择其中一个图像作为目标载体图像C，设目标载体图像C的像素值为c×c，设定待嵌入的秘密信息S为一组长度为L的字符串s，记字符串s中第i个字符为s_i，$1 \leqslant i \leqslant L$；

[0027] (5-2) 统计字符串s中各字符出现的次数，并计算出各字符的出现概率，记字符s_i的出现概率为$p(s_i)$，$0 < p(s_i) \leqslant 1$；

[0028] (5-3) 根据各字符出现概率从小到大的顺序，对各字符进行重新排序，形成一组新的字符串s_1，并查找新的字符串s_1中出现概率最小的字符；

[0029] (5-4) 以新字符串中字符从左至右的顺序查找，将查找到的出现概率最小的字符组合相加，形成新的节点，并将形成的新节点作为整体与其他未组合的字符重新排序；

[0030] (5-5) 再次重复执行步骤(5-4)，以最终得到概率之和为1，获得最终的Huffman二叉树；根据Huffman二叉树，以从根到分支、左节点为0，右节点为1的原则，得到Huffman码表；

[0031] (5-6) 根据Huffman码表中各字符对应的编码顺序，得到待嵌入秘密信息S的编码信息数据D，其中设定编码信息数据D的长度为1，第j个信息数据为d_j，$1 \leqslant j \leqslant 1$；

[0032] (5-7) 以IP置换表，对步骤(5-6)中编码信息数据D进行重新排序，以获得置换编码信息数据D_0，其中，置换编码信息数据D_0由位于左侧的L_0数据组和位于右侧的R_0数据组组成，$D_0 = L_0R_0$，该重新排序过程包括如下步骤(a)至步骤(f)：

[0033] (a) 将编码信息数据D中第58位信息数据d_{58}作为L_0数据组的第1位，编码信息数据D中第50位信息数据d_{50}作为L_0数据组中的第2位，依此类推，得到L_0数据组为$L_0 = d_{58}d_{50}d_{42}\cdots d_8$；编码信息数据D中第57位信息数据$d_{57}$作为$R_0$数据组的第1位，编码信息数据D中第49位信息数据$d_{49}$作为$L_0$数据组中的第2位，依此类推，得到$R_0$数据组为$R_0 = d_{57}d_{49}d_{41}\cdots d_7$；将$L_0$数据组和$R_0$数据组进行组合，得到置换编码信息数据$D_1 = d_{58}d_{50}d_{42}\cdots d_8d_{57}d_{49}d_{41}\cdots d_7$；

[0034] (b) 对步骤(b)所得L_0数据组和R_0数据组中数据按照IP置换表进行IP置换和异或运算，并进行16次循环迭代，得到迭代后的L'_0数据组和R'_0数据组，并令$L'_0(t) = L_0(t)$，$R'_0 = R_0(t)$，其中，迭代公式如下：

[0035] $L_0(t) = R_0(t-1)$；$R_0(t) = L_0(t) \oplus f(R_0(t-1), k_t)$，$t = 1,2,\cdots,16$；

[0036] 其中，$L_0(t)$表示L_0数据组中第t个信息数据，$R_0(t)$表示R_0数据组中第t个信息数据，⊕表示异或运算，f(,)表示由S盒决定的置换算法，k_t表示由密钥编排产生的数据块；

[0037] IP置换表如下：

[0038]

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	3	3

61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

[0039] (c) 对步骤 (b) 所得迭代后的 L'_0数据组和 R'_0数据组中的数据按照 IP^{-1}逆置换表进行置换，得到密文数据 D'；其中，IP^{-1}逆置换表如下：

[0040]

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

[0041] (d) 将预处理后的秘密信息中每个比特按 zigzag 扫描的方式对应于载体图像 C 的各个像素值，并记录像素的 LSB 数据流；

[0042] (e) 统计每个像素的 LSB 与欲嵌入的秘密信息比特不同的像素个数，记不同的像素构成向量 g，并计算、获取最优组合 $x_0, x_1, x_2, \cdots, x_{255}$；其中，最优组合 $x_0, x_1, x_2, \cdots, x_{255}$的求解公式如下：

[0043] $$\sum_{j=2i} x_j + \sum_{j=2i+1} (g_j - x_j) = \sum_{j=2i} (g_j - x_j) + \sum_{j=2i+1} x_j$$

[0044] g' = Mx+g_s，g' 表示图像隐写后的像素矩阵；

[0045] $$x_t = \begin{cases} 0, x_t < 0 \\ g_t, x_t > g_t \\ \lfloor x_t \rfloor, 0 \le x_t \le g_t \end{cases}, \quad t = 1, 2, \cdots, 255;$$

[0046] $$d = \left\| \mathbf{g}^{*} - \mathbf{g} \right\| = \sqrt{\sum_{j=0}^{255} \left(g_j^{*} - g_j \right)^2};$$

[0047] (f) 对于灰度值为 g_j的像素点集合 ($g_0, g_1, g_2, \cdots, g_{255}$)，选择 x_j个像素将其灰度值减 1，并将剩余的 (g_j-x_j) 个像素的灰度值加 1，从而得到嵌入秘密信息 S 的加密载体图像 C'，其中，加密载体图像 C' 的像素矩阵为 g'；

[0048] (6) 定位模块获取移动终端当前所处的位置数据，并发送获取的位置数据给秘钥生成模块；

[0049] (7) 秘钥生成模块接收位置数据，以接收的位置数据作为与载密图像对应的加密秘钥，并将生成的加密秘钥发送给图像发送模块；

[0050] (8) 图像发送模块将接收的加密秘钥、载密图像以及其他帧图像一起保存到图像存储模块，秘密信息提取模块则根据预先已知的解密秘钥提取载密图像中的秘密信息。

[0051] 与现有技术相比，本发明的优点在于：智能移动终端的中央处理模块判断指纹采集模块采集的移动终端操作者的指纹信息与预设智能移动终端的合法拥有者指纹信息一致时，命令移动终端开放嵌入秘密信息的权限给移动终端的操作者，由图像提取模块提取图像存储模块中的工业图纸图像，提取的图像经图像识别模块、图像类型转换模块处理转换为动态图像后，由图像预处理模块将动态图像分成多个不同帧长的帧图像，并以其中的

一个帧图像作为载体图像，嵌密模块将秘密信息嵌入到该载体图像中，秘钥生成模块产生基于定位数据的随机数作为加密秘钥，由图像发送模块将加密秘钥、载密图像以及其他帧图像一起保存，以增加载体图像的迷惑性，从而既识别了移动终端操作者的合法身份，又安全地将秘密信息嵌入到工业图纸中，保证了秘密信息的安全。

附图说明

[0052] 图 1 为本发明实施例中基于智能移动终端图像的工业图纸加密系统的结构示意图；

[0053] 图 2 为本发明实施例中智能移动终端图像的工业图纸加密方法的流程示意图；

[0054] 图 3(a) 至图 3(d) 分别为本发明实施例中选择的载体图像“Lena”、“Baboon”、“Peppers”和“Boats”；

[0055] 图 4(a) 至图 4(d) 分别为嵌入秘密信息后的载密图像“Lena”、“Baboon”、“Peppers”和“Boats”。

具体实施方式

[0056] 以下结合附图实施例对本发明作进一步详细描述。

[0057] 如图 1 所示，本实施例中基于智能移动终端图像的工业图纸加密系统，智能移动终端包括中央处理模块 1 以及分别连接中央处理模块 1 的指纹采集处理模块 2、图像采集模块 3、图像存储模块 4、图像提取模块 5、图像类型识别模块 6、图像类型转换模块 7、图像预处理模块 8、嵌密模块 9、定位模块 10、秘钥生成模块 11、文本识别转换模块 12、图像发送模块 13 和秘密信息提取模块 14；图像存储模块 14 分别连接图像采集模块 3 和图像提取模块 5，图像预处理模块 8 分别连接图像类型识别模块 6、图像类型转换模块 7 和嵌密模块 9，定位模块 10 连接秘钥生成模块 11，文本识别转换模块 12 连接嵌密模块 9，图像发送模块 13 分别与嵌密模块 9、秘钥生成模块 11 和秘密信息提取模块 14 连接，其中，

[0058] 中央处理模块 1，根据指纹采集处理模块 2 采集到的智能移动终端操作者的指纹信息，并判断与预设智能移动终端的合法拥有者指纹信息一致时，则命令移动终端开放嵌入秘密信息的权限给移动终端的操作者，并命令连接中央处理模块 1 的各模块启动；

[0059] 指纹采集处理模块 2，用以采集智能移动终端操作者的指纹信息，并发送采集到的智能移动终端操作者的指纹信息给中央处理模块 1；

[0060] 图像采集模块 3，用以采集工业图纸为外部图像，并对采集的外部图像自动编号，存储至图像存储模块；

[0061] 图像存储模块 4，一方面保存图像采集模块编号的外部图像，一方面保存系统预先存储的图像；

[0062] 图像提取模块 5，用于提取图像存储模块中的图像，并发送给图像类型识别模块 6；

[0063] 图像类型识别模块 6，用以判断所接收的图像类型为动态图像时，则将其发送给图像预处理模块 8 处理；判断接收的图像为静态图像时，则发送图像给图像类型转换模块 7 处理；

[0064] 图像类型转换模块 7，用以将接收的静态图像转换为动态图像，并发送转换后的动

态图像给图像预处理模块 8 ；

[0065] 图像预处理模块 8，用以对接收的动态图像进行滤噪或加噪处理，并将滤噪或加噪后的动态图像分解成多个不同帧长的帧图像，并将各帧图像分别作为载体图像发送给嵌密模块 9 嵌入秘密信息 ；

[0066] 嵌密模块 9，用以将字符串形式的秘密信息嵌入到接收的滤噪或加噪后的载体图像中，并将载密图像发送给图像发送模块 13 ；

[0067] 定位模块 10，用以获取移动终端当前所处的位置数据，并发送获取的位置数据给秘钥生成模块 11 ；

[0068] 秘钥生成模块 11，接收位置数据，并以接收的位置数据作为与载密图像对应的加密秘钥，并将生成的加密秘钥发送给图像发送模块 13 ；

[0069] 文本识别转换模块 12，用于识别需要加密的信息为非字符串形式时，将非字符串形式的信息转换为字符串形式的加密信息，并发送给嵌密模块 9 ；识别需要加密的信息为字符串形式的信息时，则直接发送给嵌密模块 9 ；

[0070] 图像发送模块 13，将接收的加密秘钥、载密图像以及其他帧图像一起保存到图像存储模块 4 ；秘密信息提取模块 14，用以利用对应加密秘钥的解密秘钥提取载密图像中的秘密信息。

[0071] 以下结合图 1 和图 2，对智能移动终端图像的工业图纸加密方法作出说明。该图纸加密方法依次包括如下步骤 ：

[0072] (1) 指纹采集处理模块 2 采集智能移动终端操作者的指纹信息给中央处理模块 1，中央处理模块 1 判断采集的指纹信息与预设的智能移动终端合法拥有者的指纹信息一致时，则命令图像采集模块 3 采集外部图像后进行自动编号，并保存至图像存储模块 4 中 ；

[0073] (2) 图像提取模块 5 提取图像存储模块 4 中存储的外部图像或系统预存图像，并将提取的图像发送给图像类型识别模块 6 进行识别 ；

[0074] (3) 图像类型识别模块 6 判断图像类型为动态图像时，则将其发送给图像预处理模块 8 ；判断接收的图像为静态图像时，则发送图像给图像类型转换模块 7，由图像类型转换模块 7 将静态图像转换为动态图像，并发送给图像预处理模块 8 ；

[0075] (4) 文本识别转换模块 12 识别需要加密的信息为非字符串形式时，将非字符串形式的信息转换为字符串形式的加密信息，并发送给嵌密模块 9 ；识别需要加密的信息为字符串形式的信息时，则直接发送给嵌密模块 9 ；

[0076] (5) 图像预处理模块 8 对接收的动态图像进行滤噪或加噪处理，将滤噪或加噪后的动态图像以预设的时间段分解成多个不同帧长的帧图像，并将各帧图像分别作为待选载体图像发送给嵌密模块 9 嵌入秘密信息 ；其中，嵌密模块 9 嵌入秘密信息的隐写过程依次包括如下步骤 ：

[0077] (5-1) 在多个载体图像中选择其中一个图像作为目标载体图像 C，设目标载体图像 C 的像素值为 $c \times c$，设定待嵌入的秘密信息 S 为一组长度为 L 的字符串 s，记字符串 s 中第 i 个字符为 s_i，$1 \leqslant i \leqslant L$ ；

[0078] (5-2) 统计字符串 s 中各字符出现的次数，并计算出各字符的出现概率，记字符 s_i 的出现概率为 $p(s_i)$，$0 < p(s_i) \leqslant 1$ ；

[0079] 设待嵌入的秘密信息 S 为字符串“cabcedeacacdeddaaabaababaaabbacdebacea

da”，该字符串的长度为40，则字符“a”的出现概率为0.4，字符“b”的出现概率为0.175，字符“c”的出现概率为0.15，字符“d”的出现概率为0.15，字符“e”的出现概率为0.125；

[0080] (5-3)根据各字符出现概率从小到大的顺序，对各字符进行重新排序，形成一组新的字符串 s_1，并查找新的字符串 s_1 中出现概率最小的字符；

[0081] 例如，在字符串“cabcedeacacdeddaaabaababaaabbacdebaceada”中，根据各字符出现概率从小到大重新排序后为e(0.125)、c(0.15)、d(0.15)、b(0.175)、a(0.4)，其中，e(0.125)表示字符“e”的出现概率为0.125；得到重新排序后的新字符串为“ecdba”；

[0082] (5-4)以新字符串中字符从左至右的顺序查找，将查找到的出现概率最小的字符组合相加，形成新的节点，并将形成的新节点作为整体与其他未组合的字符重新排序；例如，在新字符串“ecdba”中，从左至右出现概率最小的字符为d(0.15)、b(0.175)、(e+c)(0.275)、a(0.4)；

[0083] (5-5)再次重复执行步骤(5-4)，以最终得到概率之和为1，获得最终的Huffman二叉树；根据Huffman二叉树，以从根到分支、左节点为0，右节点为1的原则，得到Huffman码表；

[0084] 根据此步骤的说明，可以得到各字符及对应的编码为a(0)、b(111)、c(101)、d(110)、e(100)，从而得到字符串“cabcedeacacdeddaaabaababaaabbacdebaceada”的信息编码为1010111101100……01100；

[0085] (5-6)根据Huffman码表中各字符对应的编码顺序，得到待嵌入秘密信息S的编码信息数据D，其中设定编码信息数据D的长度为1，第j个信息数据为 d_j，$1 \leqslant j \leqslant l$；

[0086] 例如，本实施例中字符串“cabcedeacacdeddaaabaababaaabbacdebaceada”的编码信息数据D为1010111101100……01100，编码信息数据的第4个信息数据为0，第5个信息数据为1；

[0087] (5-7)以IP置换表，对步骤(5-6)中编码信息数据D进行重新排序，以获得置换编码信息数据 D_0，其中，置换编码信息数据 D_0 由位于左侧的 L_0 数据组和位于右侧的 R_0 数据组组成，$D_0 = L_0R_0$，该重新排序过程包括如下步骤(a)至步骤(f)：

[0088] (a)将编码信息数据D中第58位信息数据 d_{58} 作为 L_0 数据组的第1位，编码信息数据D中第50位信息数据 d_{50} 作为 L_0 数据组中的第2位，依此类推，得到 L_0 数据组为 $L_0 = d_{58}d_{50}d_{42}\cdots d_8$；编码信息数据D中第57位信息数据 d_{57} 作为 R_0 数据组的第1位，编码信息数据D中第49位信息数据 d_{49} 作为 L_0 数据组中的第2位，依此类推，得到 R_0 数据组为 $R_0 = d_{57}d_{49}d_{41}\cdots d_7$；将 L_0 数据组和 R_0 数据组进行组合，得到置换编码信息数据 $D_1 = d_{58}d_{50}d_{42}\cdots d_8d_{57}d_{49}d_{41}\cdots d_7$；

[0089] (b)对步骤(b)所得 L_0 数据组和 R_0 数据组中数据按照IP置换表进行IP置换和异或运算，并进行16次循环迭代，得到迭代后的 L'_0 数据组和 R'_0 数据组，并令 $L'_0(t) = L_0(t)$，$R'_0 = R_0(t)$，其中，迭代公式如下：

[0090] $L_0(t) = R_0(t-1)$；$R_0(t) = L_0(t) \oplus f\left(R_0(t-1), k_t\right)$，$t = 1, 2, \cdots, 16$；

[0091] 其中，$L_0(t)$ 表示 L_0 数据组中第t个信息数据，$R_0(t)$ 表示 R_0 数据组中第t个信息数据，$\oplus$ 表示异或运算，f(,)表示由S盒决定的置换算法，k_t 表示由密钥编排产生的数据块；

[0092] IP置换表如下：

[0093]

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	3	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

[0094] (c) 对步骤 (b) 所得迭代后的 L'_0数据组和 R'_0数据组中的数据按照 IP^{-1}逆置换表进行置换，得到密文数据 D'；其中，IP^{-1}逆置换表如下：

[0095]

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

[0096] (d) 将预处理后的秘密信息中每个比特按 zigzag 扫描的方式对应于载体图像 C 的各个像素值，并记录像素的 LSB 数据流；

[0097] (e) 统计每个像素的 LSB 与欲嵌入的秘密信息比特不同的像素个数，记不同的像素构成向量 g，并计算、获取最优组合 $x_0, x_1, x_2, \cdots, x_{255}$；其中，最优组合 $x_0, x_1, x_2, \cdots, x_{255}$的求解公式如下：

[0098] $$\sum_{j=2i} x_j + \sum_{j=2i+1} (g_j - x_j) = \sum_{j=2i} (g_j - x_j) + \sum_{j=2i+1} x_j$$

[0099] $g' = Mx + g_s$，g' 表示图像隐写后的像素矩阵；

[0100] $$x_t = \begin{cases} 0, x_t < 0 \\ g_t, x_t > g_t \\ \lfloor x_t \rfloor, 0 \le x_t \le g_t \end{cases}, \quad t = 1, 2, \cdots, 255;$$

[0101] $$d = \left\| \mathbf{g}' - \mathbf{g} \right\| = \sqrt{\sum_{j=0}^{255} \left(g'_j - g_j \right)^2};$$

[0102] (f) 对于灰度值为 g_j的像素点集合 $(g_0, g_1, g_2, \cdots, g_{255})$，选择 x_j个像素将其灰度值减 1，并将剩余的 $(g_j - x_j)$ 个像素的灰度值加 1，从而得到嵌入秘密信息 S 的加密载体图像 C'，其中，加密载体图像 C' 的像素矩阵为 g'；

[0103] (6) 定位模块 10 获取移动终端当前所处的位置数据，并发送获取的位置数据给秘钥生成模块 11；

[0104] (7) 秘钥生成模块 11 接收位置数据，以接收的位置数据作为与载密图像对应的加密秘钥，并将生成的加密秘钥发送给图像发送模块 13；

[0105] (8) 图像发送模块 13 将接收的加密秘钥、载密图像以及其他帧图像一起保存到图

像存储模块 4，秘密信息提取模块 14，用以利用对应加密秘钥的解密秘钥提取载密图像中的秘密信息。

[0106] 为了解本发明中秘密信息嵌入载体图像的隐写方法的隐写性能，本实施例中对该图像隐写方法做了仿真：本方法选择大小 512×512 的 BMP 格式标准灰度图像作为仿真的载体图像，待嵌入秘密信息为“cabcedeacacdeddaaabaababaaabbacdebaceada”。其中，

[0107] 如图 3(a) 至图 3(d) 所示，四幅载体图像分别为“Lena”、“Baboon”、“Peppers”和“Boats”；利用本发明提出的图像隐写方法对上面四幅载体图像满嵌入秘密信息后分别对应得到如图 4(a) 至图 4(d) 中的四幅嵌密图像。按照对应比较的原则，由图 3 和图 4 可以看出，载体图像和嵌入秘密信息后的载密图像在主观视觉上是分辨不出差异的。这说明在智能移动终端中，本发明中的图像隐写方法具有良好的视觉隐蔽性，极大地提高了秘密信息嵌入载体图像的隐写性能。

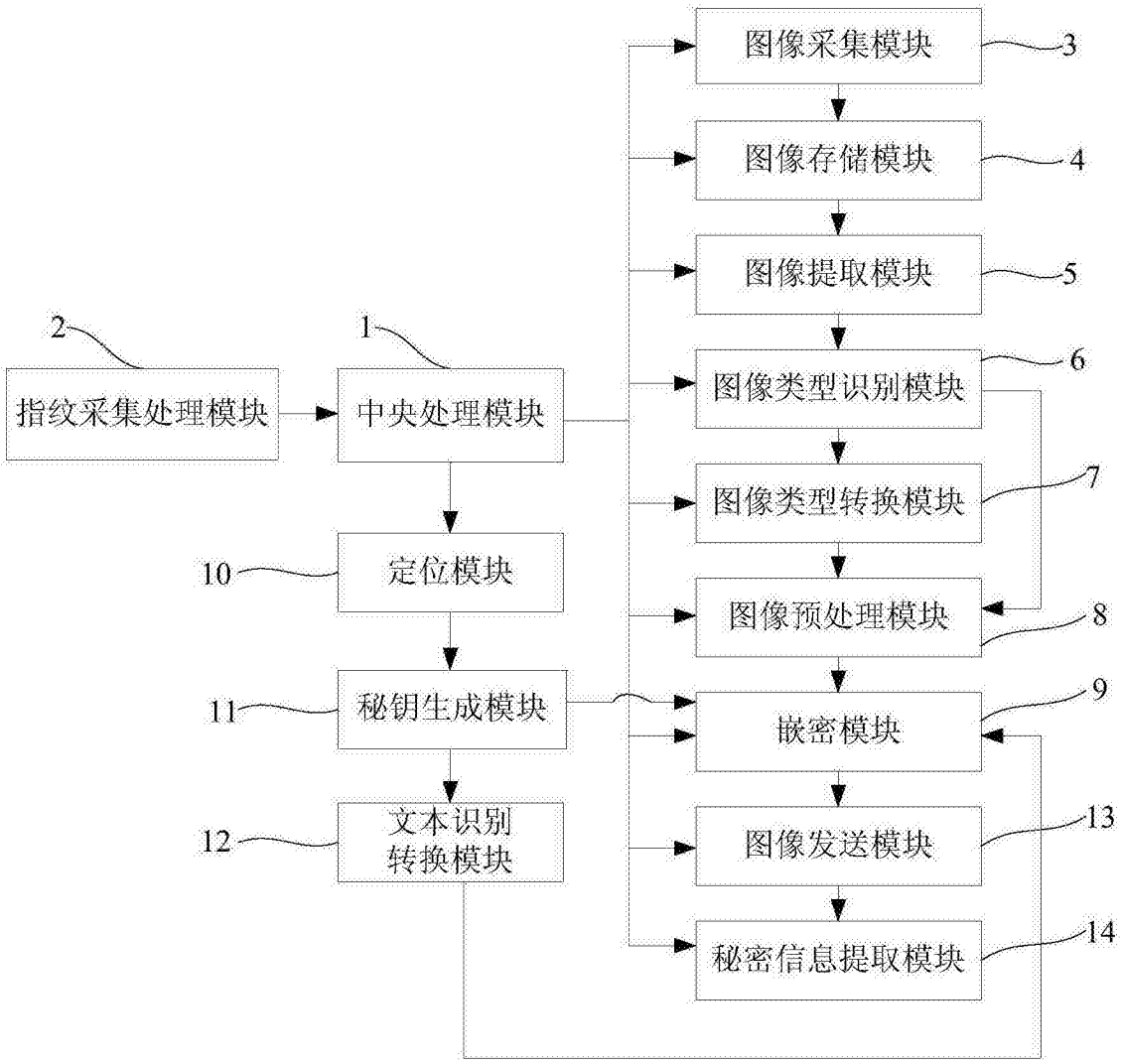

图像采集模块
3
图像存储模块
4
图像提取模块
5
2
1
6
指纹采集处理模块
中央处理模块
图像类型识别模块
图像类型转换模块
7
10
定位模块
图像预处理模块
8
11
秘钥生成模块
9
嵌密模块
文本识别
转换模块
12
图像发送模块
13
秘密信息提取模块
14

图 1

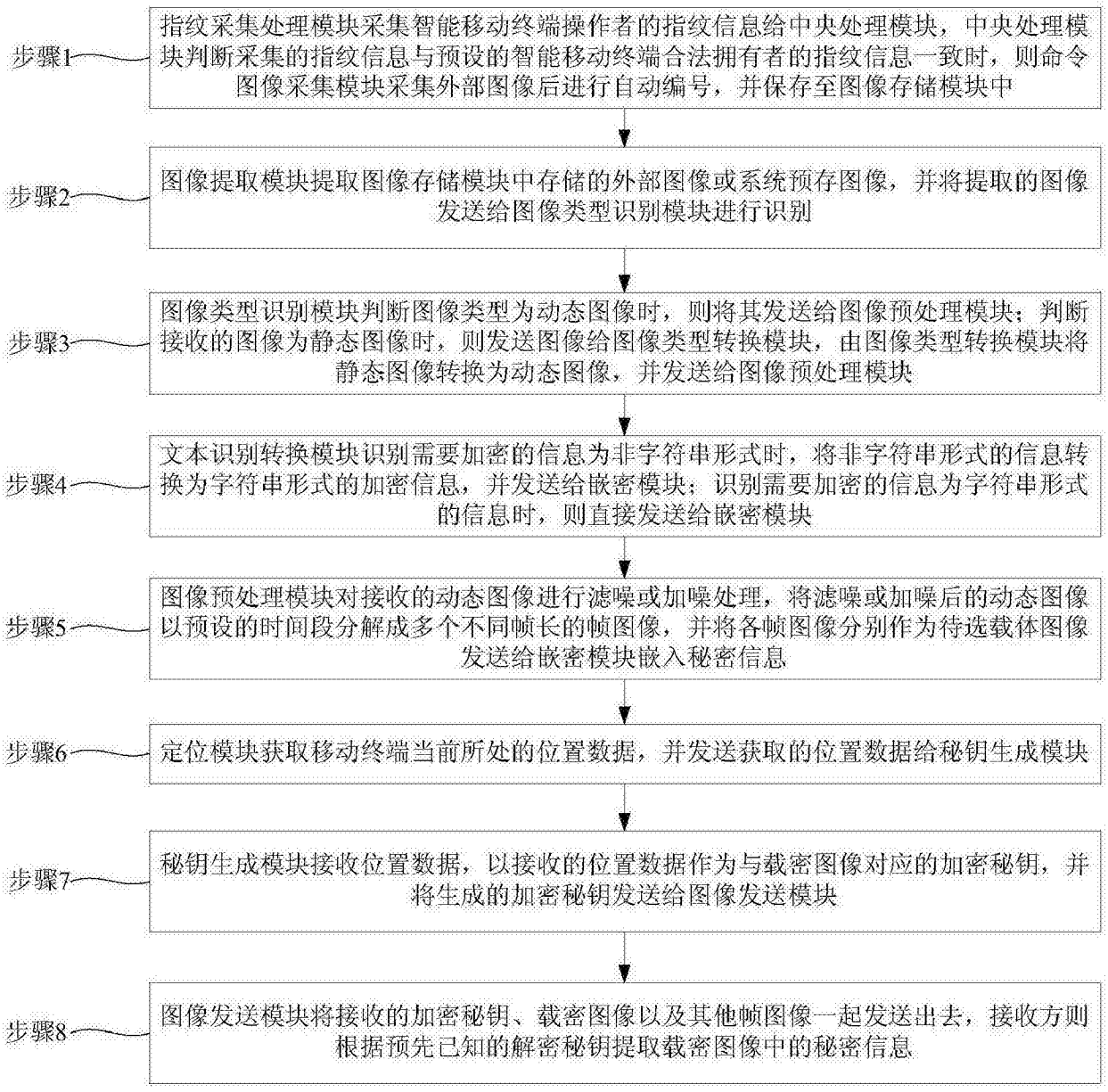
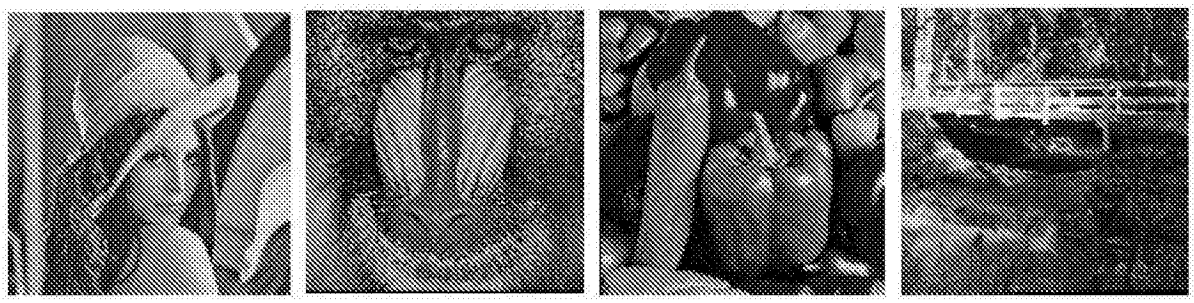
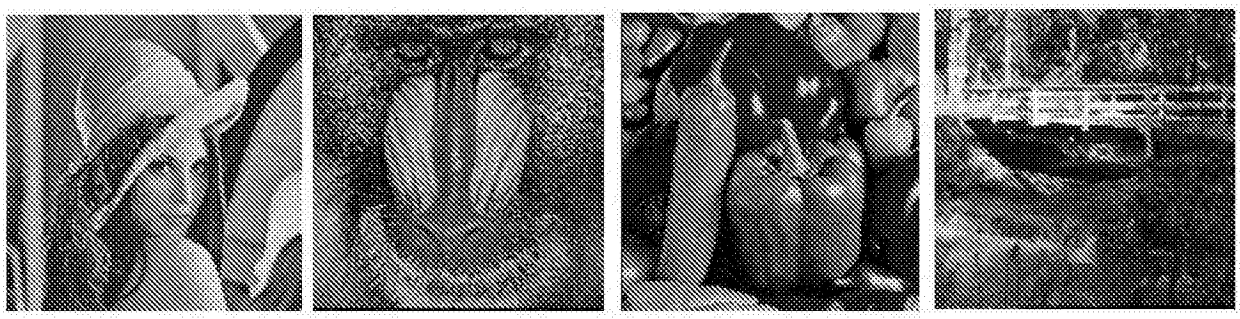

步骤1
指纹采集处理模块采集智能移动终端操作者的指纹信息给中央处理模块，中央处理模块判断采集的指纹信息与预设的智能移动终端合法拥有者的指纹信息一致时，则命令图像采集模块采集外部图像后进行自动编号，并保存至图像存储模块中
步骤2
图像提取模块提取图像存储模块中存储的外部图像或系统预存图像，并将提取的图像发送给图像类型识别模块进行识别
步骤3
图像类型识别模块判断图像类型为动态图像时，则将其发送给图像预处理模块；判断接收的图像为静态图像时，则发送图像给图像类型转换模块，由图像类型转换模块将静态图像转换为动态图像，并发送给图像预处理模块
步骤4
文本识别转换模块识别需要加密的信息为非字符串形式时，将非字符串形式的信息转换为字符串形式的加密信息，并发送给嵌密模块；识别需要加密的信息为字符串形式的信息时，则直接发送给嵌密模块
步骤5
图像预处理模块对接收的动态图像进行滤噪或加噪处理，将滤噪或加噪后的动态图像以预设的时间段分解成多个不同帧长的帧图像，并将各帧图像分别作为待选载体图像发送给嵌密模块嵌入秘密信息
步骤6
定位模块获取移动终端当前所处的位置数据，并发送获取的位置数据给秘钥生成模块
步骤7
秘钥生成模块接收位置数据，以接收的位置数据作为与载密图像对应的加密秘钥，并将生成的加密秘钥发送给图像发送模块
步骤8
图像发送模块将接收的加密秘钥、载密图像以及其他帧图像一起发送出去，接收方则根据预先已知的解密秘钥提取载密图像中的秘密信息

图 2



（a） （b） （c） （d）

图 3



(a) (b) (c) (d)

图 4