

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 2 月 13 日 (13.02.2020)



(10) 国际公布号
WO 2020/029334 A1

- (51) 国际专利分类号:
G06T 1/00 (2006.01)
- (21) 国际申请号: PCT/CN2018/102211
- (22) 国际申请日: 2018 年 8 月 24 日 (24.08.2018)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201810894261.0 2018年8月8日 (08.08.2018) CN
- (71) 申请人: 山东科技大学(SHANDONG UNIVERSITY OF SCIENCE AND TECHNOLOGY) [CN/CN]; 中国山东省青岛市黄岛区前湾港路 579 号, Shandong 266590 (CN)。
- (72) 发明人: 颜斌 (YAN, Bin); 中国山东省青岛市黄岛区前湾港路 579, Shandong 266590 (CN)。
杨红梅 (YANG, Hongmei); 中国山东省青岛市

黄岛区前湾港路 579, Shandong 266590 (CN)。
潘正祥 (PAN, Jengshyang); 中国山东省青岛市黄岛区前湾港路 579, Shandong 266590 (CN)。
陈娜 (CHEN, Na); 中国山东省青岛市黄岛区前湾港路 579, Shandong 266590 (CN)。
郝建军 (HAO, Jianjun); 中国山东省青岛市黄岛区前湾港路 579, Shandong 266590 (CN)。

(74) 代理人: 青岛智地领创专利代理有限公司 (QINGDAO ZHIDILINGCHUANG PATENT AGENCY CO., LTD); 中国山东省青岛市黄岛区香江路 110 号高科技创业中心 215 室联系人: 窦懋松, Shandong 266555 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,

(54) Title: VISUAL ENCRYPTION METHOD FOR GRAYSCALE IMAGE

(54) 发明名称: 一种灰度图像可视加密方法

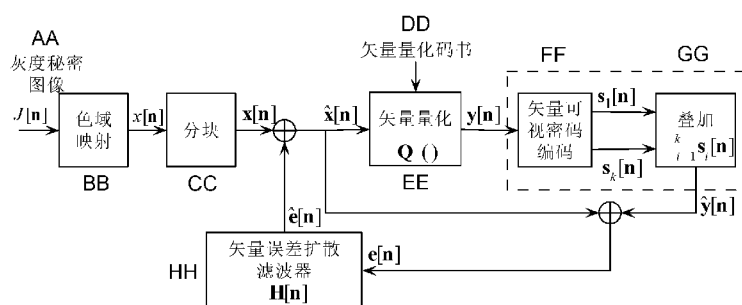


图 3

AA Grayscale secret image
BB Gamut mapping
CC Blocking
DD Vector quantization codebook
EE Vector quantization
FF Vector visual password encoding
GG Overlying
HH Vector error diffusion filter

(57) Abstract: A visual encryption method for a grayscale image. The method places, into an error diffusion feedback loop, the two processes of generating a shared image and overlaying decoding in a visual password. At an encoder end, each pixel or image block is sequentially processed according to a certain scan sequence. Inspection of an overlaying decoding effect is performed instantly on each pixel or image block of a generated shared image. A reconstructed target image acquired after overlaying and an original secret image are compared to acquire a difference therebetween. The difference is fed back and diffused to a surrounding pixel or image block that is not yet quantified, thereby improving the quality of a decoded and reconstructed secret image. An analysis process corresponds to a process of generating a shared image from a secret image. A synthetic process corresponds to a process of acquiring a target image from a shared image. The method incorporates synthesis in analysis, i.e., adopts synthesis-based analysis.

(57) 摘要: 一种灰度图像可视加密方法, 该方法将可视密码中产生分存图像和叠加解码两个过程置于一个误差扩散反馈环内。在编码器端, 按照一定扫描顺序来顺序处理每个像素或者图像块, 对产生的分存图像上的每个像素或者图像块, 即时检查其叠加解码效果, 将叠加后获得的重建目标图像和原始秘密图像对比, 获得二者的差异, 将对差异反馈并扩散到尚未量化的周围像素或者图像块上, 从而达到提高解码重建秘密图像质量的目的, 分析过程对应于从秘密图像产生分存图像过程, 而合成过程对应于从分存图像获得目标图像过程, 该方法将合成放在分析中, 即基于合成的分析。

JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,
LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区
保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告 (条约第21条(3))。

一种灰度图像可视加密方法

技术领域

本发明涉及多媒体通信安全领域，尤其涉及一种灰度图像可视加密方法。

背景技术

可视加密是一种解码过程高效且不需要任何计算的秘密分享方法，对于一个 (n, k) 阈值可视密码，它将一幅秘密图像分成 n 份传输，只有获得其中的至少 k 份，将其叠加才能恢复秘密图像的内容。近年来，视觉密码的研究有两个重点：一个是减小分存图像的尺寸，另一个是提高重建图像的视觉质量。其中，分存图像尺寸相对于秘密图像尺寸一般有扩展，小的扩展系数甚至尺寸不扩展的可视密码具备很多优势，例如处理复杂度低，占用存储空间小，占用传输带宽低等。针对二值秘密图像，典型的尺寸不变视觉密码算法包括随机网格法、概率算法和分块编码方法等三种。但是，在减小分存图像尺寸的同时，重建图像的质量却大幅下降。尤其对于灰度秘密图像，其重建图像的质量远达不到要求。

与普通二值图像视觉密码不同，灰度和彩色图像视觉密码的秘密图像是灰度和彩色图像，重建图像是呈现类似半色调的图像。聚焦到灰度图像视觉密码，当前对尺寸不扩展视觉密码（Size-Invariant Visual Cryptography）的研究可以大致划分为两类。一类是半色调化和视觉密码加密分离的方案，另一类是直接分块量化和映射的方案。其中：

第一类关于半色调化和视觉密码加密分离的方案：

首先将灰度图像转换为二值图像，例如使用半色调化或者简单的固定阈值二值量化技术，然后对此二值图像进行视觉密码编码。该方案将半色调过程和视觉加密过程分隔开：半色调化过程不考虑后续的视觉密码加密；而视觉加密的时候不考虑所处理的图像是否是半色调的，还是类似公司标识那样的二值图像。这类算法是目前灰度图像视觉密码的主流。

第二类关于直接分块量化和映射的方案：

首先将灰度图像分块，然后将每块的平均灰度量化为不同的量化级，这些量化级对应着重建图像上不同的二值模式，每个二值模式具有不同的块平均灰度，从而重建图像可通过不同二值模式来近似表达秘密图像的局部亮度和色彩。

现有的框架存在两个主要问题：

1. 不补偿重建图像上的亮度损失，
2. 不直接优化重建图像质量。

首先，从秘密像素/图像块到重建像素/图像块之间的有损映射没有被周围其他的像素和图像块补偿。由于视觉密码的安全性条件的限制，重建图像上表达秘密二值图像的能力有限。

例如,如果采用 2 乘 2 的图像块,根据块内黑像素的数量,秘密图像的图像块有 5 种,但是,在重建图像上,只允许有 3 种可能的图像块,其中黑像素的数量分别是 2、3 和 4。这样,从秘密图像块到重建图像块,存在多对一的有损映射。目前的算法都无法补偿这种亮度损失。

其次,现有算法没有直接优化重建图像的感知质量。不仅如此,虽然重建图像是半色调类型的图像,但是,现有算法所用的图像质量测度并没有反映人的视觉系统如何感知半色调图像。具体而言,重建图像的谱特性没有反映在现有的质量测度中。

现有文献中常用的质量测度是块内方差和全局对比度。块内方差测度度量了重建图像相对于秘密二值图像的均匀性。但是,它并没有度量半色调重建图像的感知质量。全局对比度测度则度量了重建图像上用于表达黑色秘密像素和白色秘密像素的图像块的亮度差异,该测度是为二值秘密图像设计的。近期,X. T. Wu 等人提出能产生蓝噪声的分存图像的视觉密码,但是,将两个蓝噪声分存图像叠加后,重建图像将不再具有蓝噪声特性,所以该类算法只适合将灰度秘密图像简单二值化后再加密,从而具有很低的细节分辨能力。

发明内容

本发明的目的在于提出一种灰度图像可视加密方法,以提高重建的目标图像的视觉质量。

本发明为了实现上述目的,采用如下技术方案:

一种灰度图像可视加密方法,包括如下步骤:

s11. 色域映射

输入秘密图像是灰度图像 $J[\mathbf{n}]$, 其中 $\mathbf{n}=[n_x, n_y]$, n_x 是像素的水平位置, n_y 是像素的垂直位置, 确定图像块的大小为 $B \times B$;

将灰度图像 $J[\mathbf{n}]$ 的色域映射到可视密码叠加重建图像(即目标图像)的色域中;

s12. 分块

将色域映射后的图像进行分块, 分割为多个互相不重叠、大小为 $B \times B$ 的图像块;

以光栅扫描的顺序依次访问各个图像块, 每次处理一个图像块;

s13. 矢量量化

对每个图像块, 使用矢量量化器量化为二值图像块, 即量化后每个像素取值为 0 或者 1;

s14. 矢量可视加密

将量化后的二值图像块, 进行矢量可视密码编码, 获得 k 个分存图像块 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$;

s15. 模拟叠加解码

将 k 个分存图像块 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$ 进行叠加, 即:

将各个分存图像块的对应像素值相乘, 进行可视密码解码, 获得目标图像块 $\hat{\mathbf{y}}[\mathbf{n}]$;

s16. 误差计算

计算矢量量化器输入图像块 $\hat{\mathbf{x}}[\mathbf{n}]$ 与目标图像块 $\hat{\mathbf{y}}[\mathbf{n}]$ 之间的误差 $\mathbf{e}[\mathbf{n}]$: $\mathbf{e}[\mathbf{n}] = \hat{\mathbf{x}}[\mathbf{n}] - \hat{\mathbf{y}}[\mathbf{n}]$;

s17. 矢量误差扩散

使用矢量误差扩散滤波器 $\mathbf{H}[\mathbf{n}]$ 将误差 $\mathbf{e}[\mathbf{n}]$ 扩散到当前图像块周围的四个图像块中;

扩散后的误差是 $\hat{\mathbf{e}}[\mathbf{n}]$, 使用误差 $\hat{\mathbf{e}}[\mathbf{n}]$ 修改上述四个图像块的输入像素值, 得到修改后的图像块 $\hat{\mathbf{x}}[\mathbf{n}] = \mathbf{x}[\mathbf{n}] + \hat{\mathbf{e}}[\mathbf{n}]$, 此修改后的图像块 $\hat{\mathbf{x}}[\mathbf{n}]$ 作为步骤 s13 中矢量量化器的输入;

s18. 利用上述步骤 s13-s17 处理每个图像块, 当处理完所有的图像块之后, 将 k 个分存图像 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$ 作为输出, 获得了可视加密方法的输出结果。

优选地, 所述步骤 s11 具体为:

s111. 计算图像块内像素数: $m = B^2$;

s112. 计算目标图像块能表示的最大亮度 $\hat{y}_{\max}$;

s113. 确定色域映射: $\mathbf{G}_A: \mathbf{x}[\mathbf{n}] = \frac{\hat{y}_{\max}}{m} \mathbf{J}[\mathbf{n}]$; 其中, $\mathbf{x}[\mathbf{n}]$ 为色域映射后的图像。

优选地, 所述步骤 s13 具体为:

s131. 对每个输入到矢量量化器的图像块 $\hat{\mathbf{x}}[\mathbf{n}]$, 按照光栅扫描的顺序依次处理各个像素;

s132. 每个像素均使用二值标量量化器量化, 量化阈值设为 1/2, 输出重建点设为 0 和 1;

s133. 将二值标量量化器的输入输出误差利用误差扩散滤波器进行扩散, 扩散到该图像块中还没有量化的其他像素上;

s134. 处理完所有像素, 输出量化后的图像块, 作为矢量量化器的输出。

优选地, 所述步骤 s14 具体为:

s141. 使用任何一种 (k, k) 阈值可视密码的基本矩阵 $\mathbf{A}_0$ 和 $\mathbf{A}_1$ 来构建基本矩阵 $\mathbf{C}_j$, 其中:

$$\mathbf{C}_j = \left[\underbrace{\mathbf{A}_0 \cdots \mathbf{A}_0}_{|D|-j} \underbrace{\mathbf{A}_1 \cdots \mathbf{A}_1}_j \right]; \quad j = 0, \dots, |D|-1;$$

D 是目标图像块中所有可能的白像素数目的集合, $|D|$ 表示集合 D 中元素数目;

s142. 根据输入秘密图像的图像块中白像素的数量, 选择矩阵 $\mathbf{C}_j$;

将矩阵 $\mathbf{C}_j$ 的列置乱, 将其每一行重新排列为 $B \times B$ 图像块, 分配给一个分存图像, 作为这个分存图像的对应图像块, 这样就获得了 k 个分存图像块 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$ 。

优选地，所述步骤 s142 中，矩阵 $\mathbf{C}_j$ 的选择方法为：

对于一个秘密图像的图像块，图像块内像素数是 m ，则所有可能白像素数集合是 $M = \{0, 1, \dots, m\}$ ；而步骤 s141 中得到的基本矩阵的集合是 $\Gamma = \{\mathbf{C}_j : j = 0, 1, \dots, |D-1|\}$ ；

据此，设计一个从 M 到 Γ 的映射 $\Phi: M \rightarrow \Gamma$ ，只需要满足：

任选的两个 $m_1, m_2 \in M$ ，以及 $\mathbf{C}_{j_1}, \mathbf{C}_{j_2} \in \Gamma$ ，当 $m_1 < m_2$ 时，必须 $j_1 \leq j_2$ ；

根据这个映射，给定秘密图像块内白像素数量，选取一个矩阵 $\mathbf{C}_j$ 。

优选地，所述步骤 s17 具体为：

s171. 邻域选择

选择当前图像块的右边、左下、下面、右下四个图像块为当前图像块的邻域；这些邻域是当前图像块误差扩散的目的地；

s172. 将误差 $\mathbf{e}[\mathbf{n}]$ 使用矢量误差扩散滤波器 $\mathbf{H}[\mathbf{n}]$ 扩散到邻域中的图像块中：

顺序访问当前图像块中的每个像素，计算重建图像像素和矢量量化器输入像素的误差，使用普通标量误差扩散滤波器将该误差扩散到当前图像块周围的像素上；

如果扩散到一个已经量化的像素上，则不改变该像素值，该像素将扩散来的误差原封不动，使用同样的标量误差扩散滤波器传递到它周围的像素上。

优选地，所述方法适用于以下三类针对二值图像设计的可视密码的任一种，即：

概率可视密码、随机格点可视密码和矢量可视密码。

本发明具有如下优点：

(1) 本发明方法可以方便地和现有的针对二值图像的概率可视密码、随机格点可视密码以及矢量可视密码中的任一种结合，构建针对灰度图像的可视密码，并可显著提高重建的目标图像的视觉质量。(2) 本发明方法满足灰度可视密码的对比度和安全性条件，只要基本的二值可视密码是完善安全的，那么该方法获得的灰度图像可视密码就是完善安全的。

附图说明

图 1 为本发明实施例中灰度图像可视加密方法的原理框图。

图 2 为本发明实施例中灰度图像可视加密方法的一种流程框图。

图 3 为本发明实施例中灰度图像可视加密方法的另一种流程框图。

图 4 为本发明实施例中使用标量量化和块内误差扩散实现矢量量化示意图。

图 5 为本发明实施例中矢量误差扩散示意图。

图 6 为本发明实施例中方法与 Wang, Yang 等人算法对比结果图。

具体实施方式

本发明的基本思想如下：

如图 1 所示，提出一个具有闭环反馈的分析-合成(Analysis-by-Synthesis, AbS) 框架的加密器，从分析-合成的角度设计视觉密码，即将秘密图像分割为分存图像的过程是其中的分析部分；而将分存图像在加密器叠加生成重建图像是其中的合成部分。

AbS 的基本含义是在加密器中（而不是在解码器中），对加密获得的分存图像解码，将解码结果作为优化视觉质量的依据。具体而言，在这个 AbS 框架中，将加密器合成的重建图像反馈到分析部分，获得当前重建像素(或图像块)与秘密像素(或图像块)之间差异，这样，半色调化过程可以仔细调整其产生的二值图像中的黑白像素的比例，从而补偿上述差异。从结构上看，将可视加密和解码移到了误差扩散半色调算法的反馈环之内。

本发明提出的 AbS 框架具有很高的灵活性，它可以和现有的三种尺寸不变可视密码结合，即可以和概率可视密码、随机格点可视密码以及矢量可视密码中的任一种结合，分别获得基于 AbS 的概率可视密码、基于 AbS 的随机格点可视密码和基于 AbS 的矢量可视密码。所获得的加密系统具有香农所定义的完善安全性（Perfect Secrecy）。

下面结合附图以及具体实施方式对本发明作进一步详细说明：

如图 3 所示，以本发明方法与矢量可视密码结合为例，说明灰度图像可视加密流程：

一种灰度图像可视加密方法，包括如下步骤：

s11. 色域映射

输入秘密图像是灰度图像 $J[\mathbf{n}]$ ，其中 $\mathbf{n}=[n_x, n_y]$ ， n_x 是像素的水平位置， n_y 是像素的垂直位置，确定图像块大小为 $B \times B$ ；

将灰度图像 $J[\mathbf{n}]$ 的色域映射到可视密码叠加重建图像（即目标图像）的色域中。

该步骤 s11 具体为：

s111. 计算图像块内像素数： $m = B^2$ 。

s112. 计算目标图像块能表示的最大亮度 $\hat{y}_{\max}$ 。

最大亮度 $\hat{y}_{\max}$ 的计算方法如下：穷举所有可能的目标图像块，对每一个图像块，计算其中白像素数量，即为该图像块的亮度，计算所有这些亮度的最大值，即为 $\hat{y}_{\max}$ 。

s113. 确定色域映射： $G_A: x[\mathbf{n}] = \frac{\hat{y}_{\max}}{m} J[\mathbf{n}]$ ；其中， $x[\mathbf{n}]$ 为色域映射后的图像。

使用上述步骤的色域映射，能够保证整个误差扩散反馈环的稳定性。

如果需要的话（例如可以是当输入秘密图像的对比度较低时），可先对输入图像进行直方

图均衡，再使用上述色域映射。

s12. 分块

将色域映射后的图像进行分块，分割为多个互相不重叠、大小为 $B \times B$ 的图像块。

以光栅扫描的顺序依次访问各个图像块，每次处理一个图像块。

s13. 矢量量化

对每个图像块，使用矢量量化器量化为二值图像块，即量化后每个像素取值为 0 或者 1。

该步骤 s13 具体为：

s131. 对每个输入到矢量量化器的图像块 $\hat{\mathbf{x}}[\mathbf{n}]$ ，按照光栅扫描的顺序依次处理各个像素。

s132. 对每个像素均使用二值量化器量化，量化阈值设为 $1/2$ ，输出重建点设为 0 和 1。

s133. 将二值标量量化器的输入输出误差利用误差扩散滤波器进行扩散，扩散到该图像块中还没有量化的其他像素上。

s134. 处理完所有像素，输出量化后的图像块，作为矢量量化器的输出。

使用矢量量化器，能够以复杂度较低的标量量化和误差扩散实现复杂度较高的矢量量化。

s14. 矢量可视加密

将量化后的二值图像块，进行矢量可视密码编码，获得 k 个分存图像块 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$ 。

该步骤 s14 具体为：

s141. 使用任何一种 (k, k) 阈值可视密码的基本矩阵 $\mathbf{A}_0$ 和 $\mathbf{A}_1$ 来构建基本矩阵 $\mathbf{C}_j$ ，其中：

$$\mathbf{C}_j = \left[\underbrace{\mathbf{A}_0 \cdots \mathbf{A}_0}_{|D|-j} \underbrace{\mathbf{A}_1 \cdots \mathbf{A}_1}_j \right]; \quad j = 0, \dots, |D|-1.$$

D 是目标图像块中所有可能的白像素数目的集合， $|D|$ 表示集合 D 中元素数目。

s142. 根据输入秘密图像的图像块中白像素的数量，选择矩阵 $\mathbf{C}_j$ 。

矩阵 $\mathbf{C}_j$ 的选择方法为：

对于一个秘密图像的图像块，图像块内像素数是 m ，则所有可能白像素数集合是 $M = \{0, 1, \dots, m\}$ ；而步骤 s141 中得到的基本矩阵的集合是 $\Gamma = \{\mathbf{C}_j : j = 0, 1, \dots, |D|-1\}$ 。

据此，设计一个从 M 到 Γ 的映射 $\Phi: M \rightarrow \Gamma$ ，只需要满足：

任选的两个 $m_1, m_2 \in M$ ，以及 $\mathbf{C}_{j_1}, \mathbf{C}_{j_2} \in \Gamma$ ，当 $m_1 < m_2$ 时，必须 $j_1 \leq j_2$ 。

根据这个映射，给定秘密图像块内白像素数量，选取一个矩阵 $\mathbf{C}_j$ 。

例如，当 $M = \{0, 1, \dots, 4\}$ ， $\Gamma = \{\mathbf{C}_j : j = 0, 1, 2\}$ ，可以使用表 1 的映射，即满足上述条件。

表 1

m	$\Phi(m)$
0	0
1	0
2	1
3	2
4	2

使用这个映射，能够保证白像素多的秘密图像块对应于白像素多的目标图像块。

将矩阵 $\mathbf{C}_j$ 的列置乱，将其每一行重新排列为 $B \times B$ 图像块，分配给一个分存图像，作为这个分存图像的对应图像块，这样就获得了 k 个分存图像块 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$ 。

使用该构建方案，能够根据目标图像中白像素数目，设计出符合要求的基本矩阵。

s15. 模拟叠加解码

将 k 个分存图像块 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$ 进行叠加，即：

将各个分存图像块的对应像素值相乘，进行可视密码解码，获得目标图像块 $\hat{\mathbf{y}}[\mathbf{n}]$ 。

s16. 误差计算

计算矢量量化器输入图像块 $\hat{\mathbf{x}}[\mathbf{n}]$ 与目标图像块 $\hat{\mathbf{y}}[\mathbf{n}]$ 之间的误差 $\mathbf{e}[\mathbf{n}]$ ： $\mathbf{e}[\mathbf{n}] = \hat{\mathbf{x}}[\mathbf{n}] - \hat{\mathbf{y}}[\mathbf{n}]$ 。

s17. 矢量误差扩散

使用矢量误差扩散滤波器 $\mathbf{H}[\mathbf{n}]$ 将误差 $\mathbf{e}[\mathbf{n}]$ 扩散到当前图像块周围的四个图像块中；

扩散后的误差是 $\hat{\mathbf{e}}[\mathbf{n}]$ ，使用误差 $\hat{\mathbf{e}}[\mathbf{n}]$ 修改上述四个图像块的输入像素值，得到修改后的图像块 $\hat{\mathbf{x}}[\mathbf{n}] = \mathbf{x}[\mathbf{n}] + \hat{\mathbf{e}}[\mathbf{n}]$ ，此修改后的图像块 $\hat{\mathbf{x}}[\mathbf{n}]$ 作为步骤 s13 中矢量量化器的输入。

该步骤 s17 具体为：

s171. 邻域选择

选择当前图像块的右边、左下、下面、右下四个图像块为当前图像块的邻域，这些邻域是当前图像块误差扩散的目的地。

s172. 将误差 $\mathbf{e}[\mathbf{n}]$ 使用矢量误差扩散滤波器 $\mathbf{H}[\mathbf{n}]$ 扩散到邻域中的图像块中：

顺序访问当前图像块中的每个像素，计算重建图像像素和矢量量化器输入像素的误差，使用普通标量误差扩散滤波器将该误差扩散到当前图像块周围的像素上；

该普通标量误差扩散滤波器例如采用常用的 Floyd-Steinberg 滤波器。

如果扩散到一个已经量化的像素上，则不改变该像素值，该像素将扩散来的误差原封不动，使用同样的标量误差扩散滤波器传递到它周围的像素上。

使用该方案，能够用一系列复杂度低的标量误差扩散实现高维的矢量误差扩散。

s18. 利用上述步骤 s13-s17 处理每个图像块，当处理完所有的图像块之后，将分存图像 $s_1[n], \dots, s_k[n]$ 作为输出，获得了可视加密方法的输出结果。

通过上述流程，使得本发明方法与矢量可视密码有机结合，构建针对灰度图像的可视密码，并可显著提高重建的目标图像的视觉质量。

在进行矢量量化的过程中，使用标量量化器结合块内误差扩散来实现。这个实现的示意图如图 4 所示。斜线框内表示已量化的像素，白色框内表示尚未量化，从左往右依次处理。

针对矢量误差扩散，可使用序贯标量量化和误差扩散实现，如图 5 所示。

从图 5 (a) 到图 5 (d) 依次量化当前图像块（斜线框）内的每个像素，并将量化误差扩散和传递到当前图像块内和当前图像块外尚未量化的像素上。

使用基本矩阵构建方法，针对 $k=2, m=4$ ，获得的基本矩阵如下：

$$\mathbf{C}_0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \mathbf{C}_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \mathbf{C}_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}。$$

类似的，对于 $k=3, m=4$ ，可获得如下的基本矩阵：

$$\mathbf{C}_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \mathbf{C}_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}。$$

目标图像的质量，发明人与现有的两种算法做了比较，分别是：

- 1) D. S. Wang, F. Yi, and X. B. Li, "Probabilistic visual secret sharing schemes for grey-scale images and color images," Inform. Sci., vol. 181, no. 11, pp. 2189–2208, Jun. 2011.
- 2) C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognition Lett., vol. 25, no. 4, pp. 481–494, Mar. 2004.

与 Wang, Yang 等人算法对比，本发明目标图像的质量具有显著性能提升，如图 6 所示。

图 6 (a) 为三种方法在 PSNR 性能上的对比，图 6 (b) 为三种方法在 MSSIM 性能上的对比。

在对比时使用了 Kodak 数据库中 24 幅自然图像，横坐标 Image index 是 24 幅图像的索引。

从图 6 可以看出，本发明方法无论是 HPSNR (Human Peak Signal to Noise Ratio, 峰值信噪比) 还是 MSSIM (Mean Structural Similarity Measure, 结构相似度) 都有显著提升。

如图 2 所示，本发明实施例还针对概率可视密码或者随机网格可视密码，给出了分析-

合成框架的具体实施例子，其中，图像块的大小是 $B=1$ 。

从图 2 与图 3 对比可以看出，针对概率可视密码或者随机网格可视密码的灰度图像可视加密方法的流程与针对矢量可视密码的灰度图像可视加密方法的流程是一致的。

主要区别在于图 2 中的概率可视密码或者随机网格可视密码，其图像块的大小是 $B=1$ ，这样每个图像块就变成了一个像素块。由此，可视加密和解密部分都是针对每个像素进行的，而不是像图 3 那样针对一个图像块进行。另外，在图 2 中，量化和扩散也是针对像素进行的，而在图 3 中，量化具体是矢量量化，扩散也是矢量扩散，即扩散到周围的图像块中。

当然，以上说明仅仅为本发明的较佳实施例，本发明并不限于列举上述实施例，应当说明的是，任何熟悉本领域的技术人员在本说明书的教导下，所做出的所有等同替代、明显变形形式，均落在本说明书的实质范围之内，理应受到本发明的保护。

权 利 要 求 书

1. 一种灰度图像可视加密方法，其特征在于，包括如下步骤：

s11. 色域映射

输入秘密图像是灰度图像 $J[\mathbf{n}]$ ，其中 $\mathbf{n}=[n_x, n_y]$ ， n_x 是像素的水平位置， n_y 是像素的垂直位置，确定图像块的大小为 $B \times B$ ；

将灰度图像 $J[\mathbf{n}]$ 的色域映射到可视密码叠加重建图像（即目标图像）的色域中；

s12. 分块

将色域映射后的图像进行分块，分割为多个互相不重叠、大小为 $B \times B$ 的图像块；

以光栅扫描的顺序依次访问各个图像块，每次处理一个图像块；

s13. 矢量量化

对每个图像块，使用矢量量化器量化为二值图像块，即量化后每个像素取值为 0 或者 1；

s14. 矢量可视加密

将量化后的二值图像块，进行矢量可视密码编码，获得 k 个分存图像块 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$ ；

s15. 模拟叠加解码

将 k 个分存图像块 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$ 进行叠加，即：

将各个分存图像块的对应像素值相乘，进行可视密码解码，获得目标图像块 $\hat{\mathbf{y}}[\mathbf{n}]$ ；

s16. 误差计算

计算矢量量化器输入图像块 $\hat{\mathbf{x}}[\mathbf{n}]$ 与目标图像块 $\hat{\mathbf{y}}[\mathbf{n}]$ 之间的误差 $\mathbf{e}[\mathbf{n}]$ ： $\mathbf{e}[\mathbf{n}] = \hat{\mathbf{x}}[\mathbf{n}] - \hat{\mathbf{y}}[\mathbf{n}]$ ；

s17. 矢量误差扩散

使用矢量误差扩散滤波器 $\mathbf{H}[\mathbf{n}]$ 将误差 $\mathbf{e}[\mathbf{n}]$ 扩散到当前图像块周围的四个图像块中；

扩散后的误差是 $\hat{\mathbf{e}}[\mathbf{n}]$ ，使用误差 $\hat{\mathbf{e}}[\mathbf{n}]$ 修改上述四个图像块的输入像素值，得到修改后的图像块 $\hat{\mathbf{x}}[\mathbf{n}] = \mathbf{x}[\mathbf{n}] + \hat{\mathbf{e}}[\mathbf{n}]$ ，此修改后的图像块 $\hat{\mathbf{x}}[\mathbf{n}]$ 作为步骤 s13 中矢量量化器的输入；

s18. 利用上述步骤 s13-s17 处理每个图像块，当处理完所有的图像块之后，将 k 个分存图像 $\mathbf{s}_1[\mathbf{n}], \dots, \mathbf{s}_k[\mathbf{n}]$ 作为输出，获得了可视加密方法的输出结果。

2. 根据权利要求 1 所述的灰度图像可视加密方法，其特征在于，

所述步骤 s11 具体为：

s111. 计算图像块内像素数： $m = B^2$ ；

s112. 计算目标图像块能表示的最大亮度 $\hat{y}_{\max}$ ；

s113. 确定色域映射: $G_A: x[n] = \frac{\ddot{y}_{\max}}{m} J[n]$; 其中, $x[n]$ 为色域映射后的图像。

3. 根据权利要求 1 所述的灰度图像可视加密方法, 其特征在于,
所述步骤 s13 具体为:

s131. 对每个输入到矢量量化器的图像块 $\hat{x}[n]$, 按照光栅扫描的顺序依次处理各个像素;

s132. 每个像素均使用二值标量量化器量化, 量化阈值设为 1/2, 输出重建点设为 0 和 1;

s133. 将二值标量量化器的输入输出误差利用误差扩散滤波器进行扩散, 扩散到该图像块中还没有量化的其他像素上;

s134. 处理完所有像素, 输出量化后的图像块, 作为矢量量化器的输出。

4. 根据权利要求 1 所述的灰度图像可视加密方法, 其特征在于,
所述步骤 s14 具体为:

s141. 使用任何一种 (k, k) 阈值可视密码的基本矩阵 A_0 和 A_1 来构建基本矩阵 C_j , 其中:

$$C_j = \left[\underbrace{A_0 \cdots A_0}_{|D|-j} \underbrace{A_1 \cdots A_1}_j \right]; \quad j = 0, \dots, |D|-1;$$

D 是目标图像块中所有可能的白像素数目的集合, $|D|$ 表示集合 D 中元素数目;

s142. 根据输入秘密图像的图像块中白像素的数量, 选择矩阵 C_j ;

将矩阵 C_j 的列置乱, 将其每一行重新排列为 $B \times B$ 图像块, 分配给一个分存图像, 作为这个分存图像的对应图像块, 这样就获得了 k 个分存图像块 $s_1[n], \dots, s_k[n]$ 。

5. 根据权利要求 4 所述的灰度图像可视加密方法, 其特征在于,
所述步骤 s142 中, 矩阵 C_j 的选择方法为:

对于一个秘密图像的图像块, 图像块内像素数是 m , 则所有可能白像素数集合是 $M = \{0, 1, \dots, m\}$; 而步骤 s141 中得到的基本矩阵的集合是 $\Gamma = \{C_j : j = 0, 1, \dots, |D|-1\}$;

据此, 设计一个从 M 到 Γ 的映射 $\Phi: M \rightarrow \Gamma$, 只需要满足:

任选的两个 $m_1, m_2 \in M$, 以及 $C_{j_1}, C_{j_2} \in \Gamma$, 当 $m_1 < m_2$ 时, 必须 $j_1 \leq j_2$;

根据这个映射, 给定秘密图像块内白像素数量, 选取一个矩阵 C_j 。

6. 根据权利要求 1 所述的灰度图像可视加密方法, 其特征在于,
所述步骤 s17 具体为:

s171. 邻域选择

选择当前图像块的右边、左下、下面、右下四个图像块为当前图像块的邻域；这些邻域是当前图像块误差扩散的目的地；

s172. 将误差 $e[n]$ 使用矢量误差扩散滤波器 $H[n]$ 扩散到邻域中的图像块中：

顺序访问当前图像块中的每个像素，计算重建图像像素和矢量量化器输入像素的误差，使用普通标量误差扩散滤波器将该误差扩散到当前图像块周围的像素上；

如果扩散到一个已经量化的像素上，则不改变该像素值，该像素将扩散来的误差原封不动，使用同样的标量误差扩散滤波器传递到它周围的像素上。

7. 根据权利要求 1 至 6 任一项所述的灰度图像可视加密方法，其特征在于，

所述方法适用于以下三类针对二值图像设计的可视密码的任一种，即：

概率可视密码、随机格点可视密码和矢量可视密码。

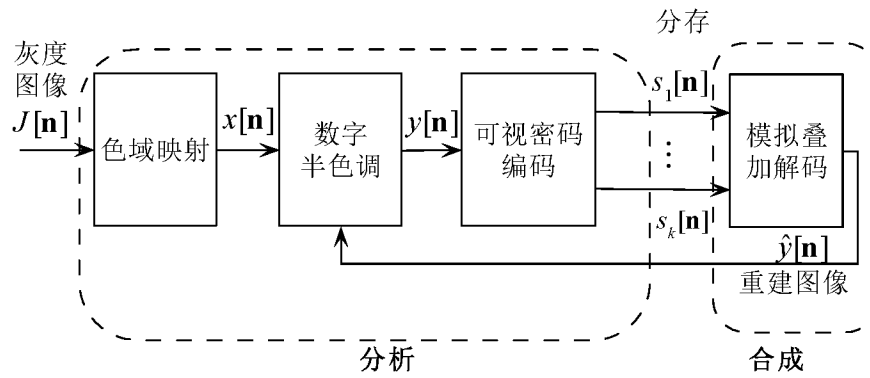


图 1

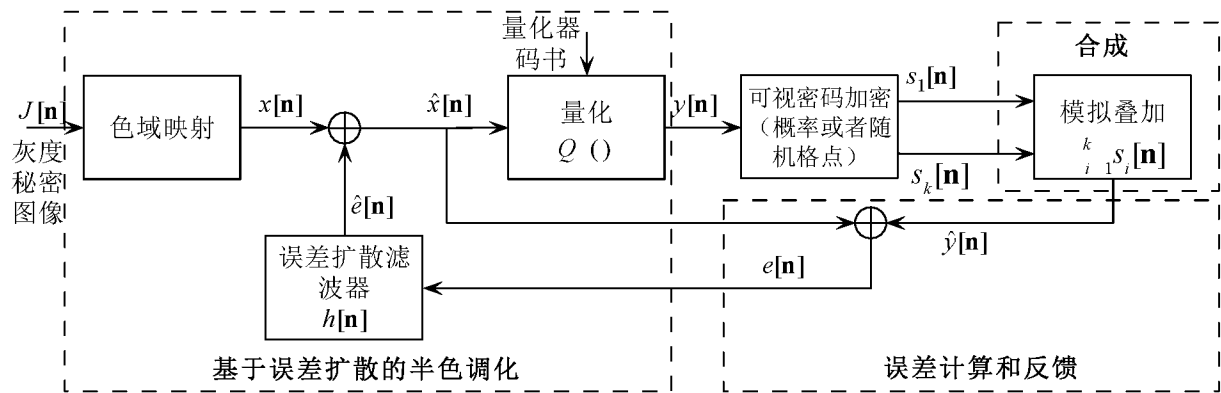


图 2

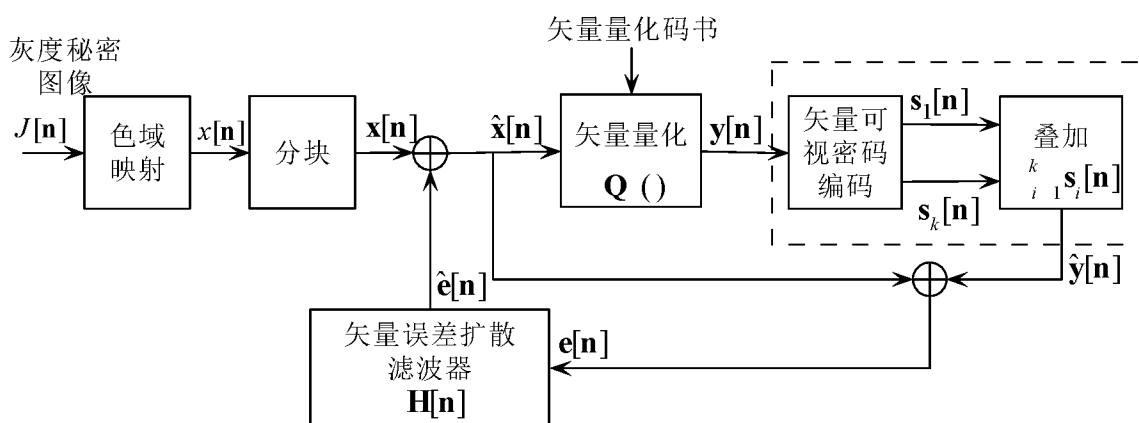


图 3

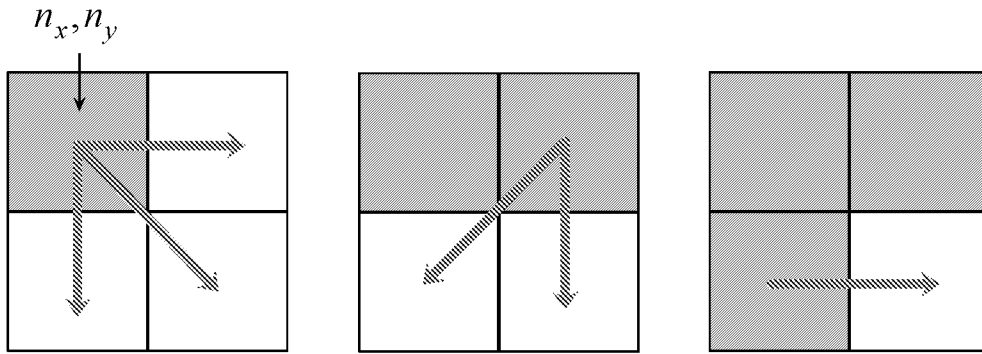


图 4

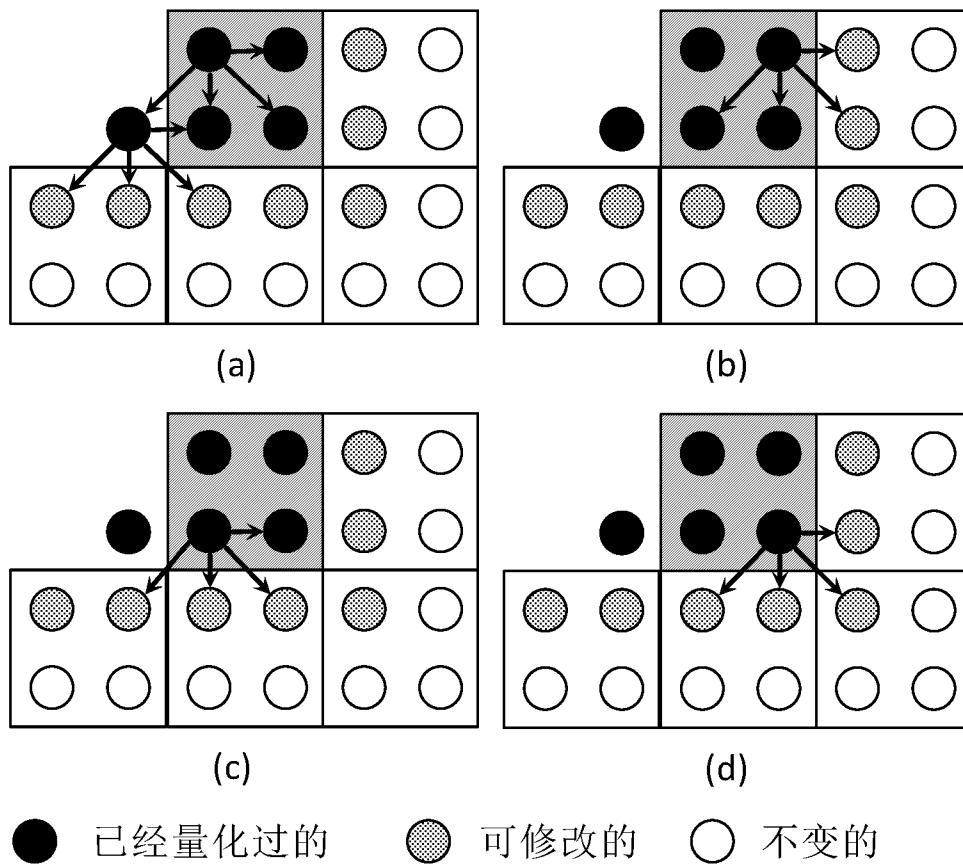


图 5

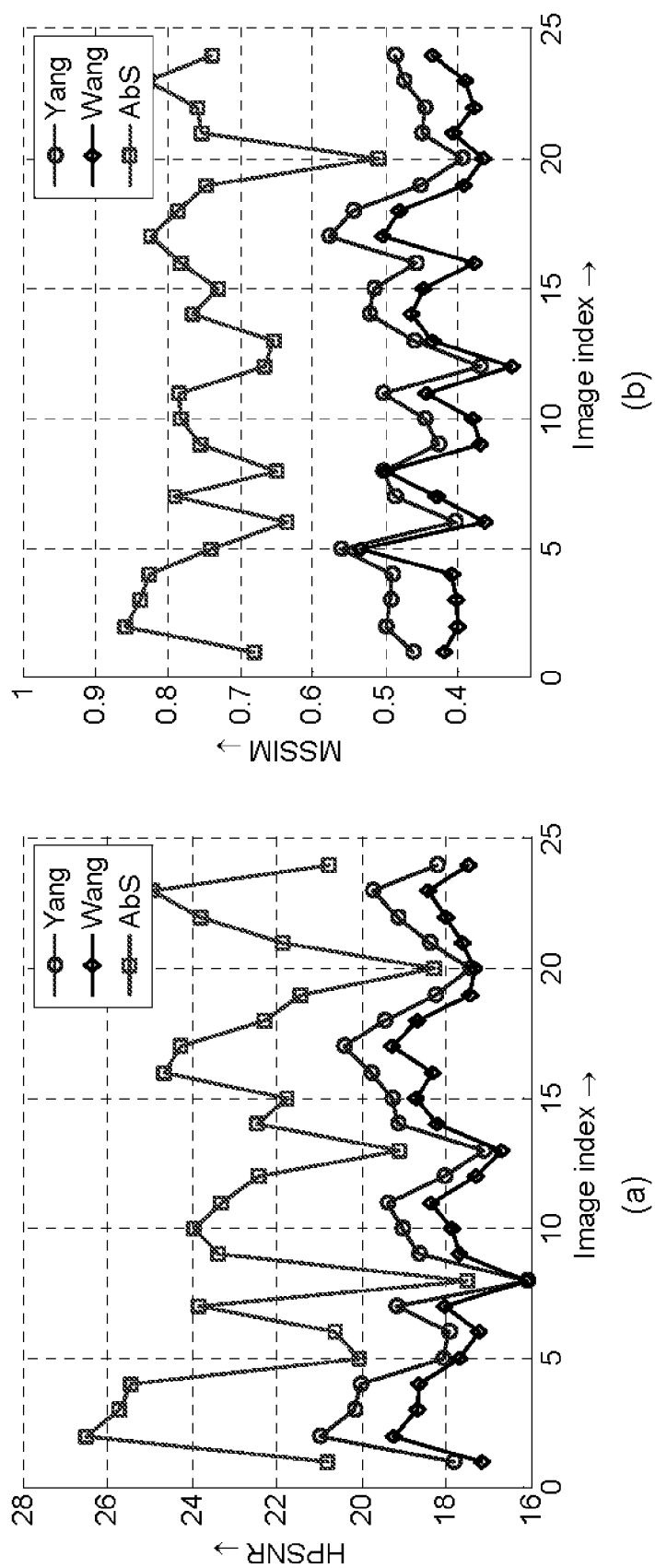


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/102211

A. CLASSIFICATION OF SUBJECT MATTER

G06T 1/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06T

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC, BAIDU: 图像, 加密, 映射, 分存, 块, 量化, 误差扩散, 叠加, image, encrypted, mapping, separated-storage, block, error-diffusion, stack

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104463767 A (SHANDONG UNIVERSITY OF SCIENCE AND TECHNOLOGY) 25 March 2015 (2015-03-25) description, paragraphs [0039]-[0065]	1-7
A	CN 104574262 A (SHANDONG UNIVERSITY OF SCIENCE AND TECHNOLOGY) 29 April 2015 (2015-04-29) entire document	1-7
A	CN 105404817 A (XIDIAN UNIVERSITY) 16 March 2016 (2016-03-16) entire document	1-7
A	CN 101751658 A (TSINGHUA UNIVERSITY) 23 June 2010 (2010-06-23) entire document	1-7
A	US 2011194727 A1 (NATIONAL TAIWAN UNIVERSITY OF SCIENCE & TECHNOLOGY) 11 August 2011 (2011-08-11) entire document	1-7



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

01 April 2019

Date of mailing of the international search report

05 May 2019

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC (ISA/CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/102211

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104463767	A	25 March 2015	None			
CN	104574262	A	29 April 2015	None			
CN	105404817	A	16 March 2016	None			
CN	101751658	A	23 June 2010	None			
US	2011194727	A1	11 August 2011	TW	201128574	A	16 August 2011

国际检索报告

国际申请号

PCT/CN2018/102211

A. 主题的分类

G06T 1/00 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

G06T

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNKI, CNPAT, WPI, EPODOC, BAIDU: 图像, 加密, 映射, 分存, 块, 量化, 误差扩散, 叠加, image, encrypted, mapping, separated-storage, block, error-diffusion, stack

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 104463767 A (山东科技大学) 2015年 3月 25日 (2015 - 03 - 25) 说明书第[0039]-[0065]段	1-7
A	CN 104574262 A (山东科技大学) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-7
A	CN 105404817 A (西安电子科技大学) 2016年 3月 16日 (2016 - 03 - 16) 全文	1-7
A	CN 101751658 A (清华大学) 2010年 6月 23日 (2010 - 06 - 23) 全文	1-7
A	US 2011194727 A1 (NATIONAL TAIWAN UNIVERSITY OF SCIENCE & TECHNOLOGY) 2011年 8月 11日 (2011 - 08 - 11) 全文	1-7

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2019年 4月 1日

国际检索报告邮寄日期

2019年 5月 5日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

穆滢

传真号 (86-10) 62019451

电话号码 86-(10)-53961531

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/102211

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104463767	A	2015年 3月 25日	无			
CN	104574262	A	2015年 4月 29日	无			
CN	105404817	A	2016年 3月 16日	无			
CN	101751658	A	2010年 6月 23日	无			
US	2011194727	A1	2011年 8月 11日	TW	201128574	A	2011年 8月 16日