(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 6 月 11 日 (11.06.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/114308 A1

(51) 国际专利分类号:
H04N 1/32 (2006.01)

(21) 国际申请号: PCT/CN2019/121557

(22) 国际申请日: 2019 年 11 月 28 日 (28.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811488248.1 2018年12月6日 (06.12.2018) CN

(71) 申请人: 中国科学院深圳先进技术研究院 (**SHENZHEN INSTITUTES OF ADVANCED TECHNOLOGY CHINESE ACADEMY OF SCIENCES**) [CN/CN]; 中国广东省深圳市深圳大学城学苑大道 1068 号, Guangdong 518055 (CN)。

(72) 发明人: **杨建权(YANG, Jianquan)**; 中国广东省深圳市深圳大学城学苑大道1068号, Guangdong 518055 (CN)。 **黄倩(HUANG, Qian)**; 中国广东省深圳市深圳大学城学苑大道1068号, Guangdong 518055 (CN)。 **张玉兰(ZHANG, Yulan)**; 中国广东省深圳市深圳大学城学苑大道1068号, Guangdong 518055 (CN)。 **常杰(CHANG, Jie)**; 中国广东省深圳市深圳大学城学苑大道1068号, Guangdong 518055 (CN)。 **朱国普(ZHU, Guopu)**; 中国广东省深圳市深圳大学城学苑大道1068号, Guangdong 518055 (CN)。

(74) 代理人: **北京市诚辉律师事务所 (BEIJING CHENGHUI LAW FIRM)**; 中国北京市朝阳区朝阳北路99号楼2单元905, Beijing 100123 (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, 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,

WO 2020/114308 A1

(54) **Title:** IMAGE ENCRYPTION AND CORRECTION METHOD AND DEVICE, AND IMAGE DECRYPTION METHOD AND DEVICE

(54) **发明名称:** 一种图像加密与校正方法、装置及图像解密方法、装置

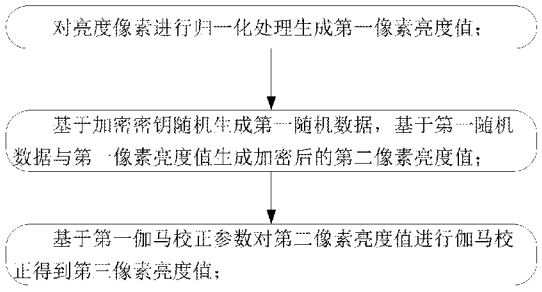


图 2

AA PERFORM NORMALIZATION PROCESSING ON BRIGHTNESS PIXELS TO GENERATE A FIRST PIXEL BRIGHTNESS VALUE

BB RANDOMLY GENERATE FIRST RANDOM DATA ON THE BASIS OF AN ENCRYPTION KEY, AND GENERATE AN ENCRYPTED SECOND PIXEL BRIGHTNESS VALUE ON THE BASIS OF THE FIRST RANDOM DATA AND THE FIRST PIXEL BRIGHTNESS VALUE

CC PERFORM GAMMA CORRECTION ON THE SECOND PIXEL BRIGHTNESS VALUE ON THE BASIS OF A FIRST GAMMA CORRECTION PARAMETER TO OBTAIN A THIRD PIXEL BRIGHTNESS VALUE

(57) **Abstract:** The present invention relates to the technical field of image processing, and provides an image encryption and correction method and device, and an image decryption method and device. The method comprises: performing normalization processing on brightness pixels to generate a first pixel brightness value; randomly generating first random data on the basis of an encryption key, and generating an encrypted second pixel brightness value on the basis of the first random data and the first pixel brightness value; and performing gamma correction on the second pixel brightness value on the basis of a first gamma correction parameter to obtain a third pixel brightness value. The generating of the encrypted second pixel brightness value on the basis of the first random data and the first pixel brightness value comprises: performing logarithmic operation on a product of the first random data and the first pixel brightness value so as to generate the encrypted second pixel brightness value. By means of the present solution, gamma correction processing can be performed on encrypted image data, thereby improving the image quality while protecting the privacy of an image of a user side, and ensuring safety of user data.

[见续页]

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))。

(57) 摘要：本发明提供一种图像加密与校正方法、装置及图像解密方法、装置，属于图像处理技术领域。该方法包括：对亮度像素进行归一化处理生成第一像素亮度值；基于加密密钥随机生成第一随机数据，基于第一随机数据与第一像素亮度值生成加密后的第二像素亮度值；基于第一伽马校正参数对第二像素亮度值进行伽马校正得到第三像素亮度值；所述基于第一随机数据与第一像素亮度值的生成加密后的第二像素亮度值，包括：对第一随机数据与第一像素亮度值的乘积进行对数运算，从而生成加密后的第二像素亮度值。通过本方案，对加密图像数据即可执行伽马校正处理提高了图像质量且保护了用户端图像的私密性，保证用户数据安全。

一种图像加密与校正方法、装置及图像解密方法、装置

技术领域

本申请涉及一种图像处理技术领域，特别是涉及一种图像加密与校正方法、装置及图像解密方法、装置。

背景技术

在社交平台上，用户希望对私人图片进行加密，以保护个人隐私；同时也希望社交平台能够对加密图像进行一定清晰化或美化处理。作为满足这一需求的关键技术，加密域信号处理技术近年来得到迅猛发展和广泛关注。

目前，对于图像进行清晰化或美化处理一般使用图像解密后基于像素域进行的图像处理，其中被广泛采用的伽马校正是常见的增强视觉质量的图像处理技术之一，其通过将亮度值根据指定的幂函数进行重新映射，可提亮过暗区域，抑制过亮区域，从而增强图像或视频的细节信息。现有技术中，一般通过公式：$y = 255 * (x/255)^{\gamma}$实现伽马校正，其中，$y$为伽马校正后的像素值，$x$为原始亮度值（0 表示最暗，255 表示最亮，$0 \le x \le 255$），$y$为伽马校正后的亮度值，$\gamma$为伽马校正的参数（$\gamma > 0$）；说明书附图 1 给出了伽马校正的效果，可以看出，伽马校正可以增强图像或视频的细节信息。然而，上述传统的伽马校正方案都是建立在对解密图像上进行的伽马校正。而一旦用户端对图像进行加密、上传后，平台端在不进行解密的情况下根本无法对于图像进行伽马校正处理，使得图像质量无法提高；另一方面，一旦平台端解密进行图像处理，这也即将大大破坏用户端图像的私密性，不能保证用户数据安全。

发明内容

为解决上述技术问题，本发明实施例提供了一种加密域伽马校正的方法及系统，保护用户私密性的情况下进行图像细节增强处理，技术方案如下：

一种图像加密与校正方法，其特征在于，包括：

对亮度像素进行归一化处理生成第一像素亮度值；

基于加密密钥随机生成第一随机数据，基于第一随机数据与第一像素亮度值生成加密后的第二像素亮度值；

基于第一伽马校正参数对第二像素亮度值进行伽马校正得到第三像素亮度

值；所述基于第一随机数据与第一像素亮度值的生成加密后的第二像素亮度值，包括：对第一随机数据与第一像素亮度值的乘积进行对数运算，从而生成加密后的第二像素亮度值。

相应的，所述第一随机数据为随机正浮点数。

相应的，所述基于第一伽马校正参数对第二像素亮度值进行伽马校正，包括：通过第一伽马校正参数与第二像素亮度值相乘，获得校正后的亮度值。

一种图像解密方法，其特征在于，包括：获得第一随机数据、第一伽马校正参数以及第三像素亮度值；

基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值；

对第一像素亮度值进行去归一化处理，生成伽马校正后的亮度值。

基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值，包括：基于公式 $\bar{y}=\begin{cases}2^{(z-\log_2 n^{\gamma})} & if\ z \neq -\gamma * \varepsilon \\ 0 & otherwise\end{cases}$ 进行还原出第一像素亮度值；

其中，γ为第一伽马校正参数，n 为第一随机数据，z 为第三像素亮度值。

相应的，所述第一随机数据为随机正浮点数。

一种图像加密与校正装置，其特征在于，包括：

归一化模块，对亮度像素进行归一化处理生成第一像素亮度值；

加密模块，基于加密密钥随机生成第一随机数据，基于第一随机数据与第一像素亮度值生成加密后的第二像素亮度值；

伽马校正模块，基于第一伽马校正参数对第二像素亮度值进行伽马校正得到第三像素亮度值；

相应的，所述基于第一随机数据与第一像素亮度值的生成加密后的第二像素亮度值，包括：对第一随机数据与第一像素亮度值的乘积进行对数运算，从而生成加密后的第二像素亮度值。

相应的，所述第一随机数据为随机正浮点数。

相应的，基于第一伽马校正参数对第二像素亮度值进行伽马校正，包括：通过第一伽马校正参数与第二像素亮度值相乘，获得校正后的亮度值。

一种图像解密装置，其特征在于，包括：

第一获取模块，获得第一随机数据、第一伽马校正参数以及第三像素亮度值；

还原模块，基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值；

去归一化模块，对第一像素亮度值进行去归一化处理，生成伽马校正后的亮度值。

相应的，基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值，包括：基于公式$\bar{y}=\begin{cases}2^{(z-\log_2 n^{\gamma})} & if\ z\neq -\gamma*\varepsilon \\ 0 & otherwise\end{cases}$进行还原出第一像素亮度值；

其中，γ为第一伽马校正参数，n为第一随机数据，z为第三像素亮度值。

相应的，所述第一随机数据为随机正浮点数。

一种图像加密与校正系统，其特征在于，包括：所述系统包括由上述任一项所述的图像加密与校正装置以及任一项所述的图像解密装置。

本发明实施例中，在基于上述实施例方案，从而对于用户端加密、上传后的图像，在不进行解密的情况下执行伽马校正处理，一方面大大提高了使得图像质量；另一方面，由于基于解密图像数据进行伽马校正处理，保护了用户端图像的私密性，保证用户数据安全；此外，采用了对数加密方法，大大降低了相对于传统复杂函数进行图像校正的方案，大大降低了的计算量。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单的介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲， 在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图1为现有技术中伽马校正处理效果图：（a）原图； （b）以$\gamma=1/2$伽马校正后的图像（c）以$\gamma=1/4$伽马校正后的图像；

图 2 为本发明实施例一中的图像加密与校正方法流程图；

图3为本发明实施例一中的图像加密的具体细节步骤流程图；

图4为本发明实施例一中的对于加密后的图像数据执行伽马校正方法流程图；

图 5 为本发明实施例二中的图像解密方法流程图；

图 6 为本发明实施例三中的图像加密与校正装置模块图；

图 7 为本发明实施例四中的图像解密装置模块图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

实施例一

本发明实施例一种图像加密与校正方法，图像的功能是对输入的像素亮度值*x*（通常是取值在0~255的整数），在加密秘钥*K*的控制下进行加密，得到加密后的像素亮度值*c*；

如图2所示，本实施例一种图像加密与校正方法包括：

对亮度像素进行归一化处理生成第一像素亮度值；

基于加密密钥随机生成第一随机数据，基于第一随机数据与第一像素亮度值生成加密后的第二像素亮度值；

所述基于第一随机数据与第一像素亮度值的生成加密后的第二像素亮度值，包括：对第一随机数据与第一像素亮度值的乘积进行对数运算，从而生成加密后的第二像素亮度值。

具体的，如图3所示，Step 1：对x进行归一化处理，得到归一化的亮度值$\bar{x} = x/255$，可知$0 \le \bar{x} \le 1$。

具体的，Step 2：在加密秘钥*K*的控制下，生成一个取值范围在[1, N] （N由用户根据所需的加密强度来设置）的随机正浮点数*n*，根据下述加密公式得到加密后的像素亮度值*c*：

$$c = \begin{cases} \log_2(n\bar{x}) & if\ \bar{x} \neq 0 \\ -\varepsilon & otherwise \end{cases}$$

式中的$-\varepsilon$用于表示此时$\bar{x} = 0$，起标记的作用，通常取$\varepsilon = 1000$。

具体的，对于没有加密秘钥的第三方，由于无法产生正确的随机正浮点数数，因此无法由c推断出x，从而起到加密的效果。

相应地，在加密秘钥 *K* 的控制下，生成一个取值范围在[1, N] （N 由用户根

据所需的加密强度来设置）的随机正浮点数 n，是基于学术界和工业界已研究多年并已相当成熟的随机数发生器技术来生成。一般软件开发包都会提供生成随机正浮点数的函数接口。另外，只需要用相同的加密秘钥 K 来初始化该函数，就能生成相同的随机数序列。由于不同开发包的随机数生成公式均可不同，因此此处写出具体公式，反而会限制专利保护范围。具体到实施例一，本发明调用 Matlab 2016a 版本的 rand 函数来生成随机正浮点数。

基于第一伽马校正参数对第二像素亮度值进行伽马校正得到第三像素亮度值；

具体地，如图 4 所示：

加密域伽马校正模块的功能是将加密后的亮度值c进行伽马校正处理，得到加密下的伽马校正值z。

Step 1：设定伽马校正参数γ，$\gamma > 0$。

Step 2：通过下述公式实现加密域伽马校正：

$$z = \gamma * c$$

相应的，所述第一随机数据为随机正浮点数。

相应的，所述基于第一伽马校正参数对第二像素亮度值进行伽马校正，包括：通过第一伽马校正参数与第二像素亮度值相乘，获得校正后的亮度值。

实施例二

本发明实施例提供一种图像解密方法，解密的功能是根据伽马校正后的加密亮度值z和伽马校正参数γ，还原出伽马校正后的亮度值y。

本发明实施例一种图像解密方法，包括：

获得第一随机数据、第一伽马校正参数以及第三像素亮度值；

基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值；

具体地，如图 5 所示：

Step 1：根据加密秘钥 K，生成随机正浮点数 n。

相应地，本发明通过调用了 Matlab 2016a 版本的 rand 函数来生成随机正浮点数。

Step 2：根据下述解密公式还原出归一化的伽马校正亮度值$\bar{y}$：

$$\bar{y} = \begin{cases} 2^{(z-\log_2 n^{\gamma})} & if\ z \neq -\gamma * \varepsilon \\ 0 & otherwise \end{cases}$$

其中，γ为第一伽马校正参数，n 为第一随机数据，z 为第三像素亮度值。

对第一像素亮度值进行去归一化处理，生成伽马校正后的亮度值。

具体地，对$\bar{y}$进行去归一化，得到伽马校正后的亮度值y

$$y = \bar{y} * 255$$

相应的，所述第一随机数据为随机正浮点数。

实施例三

如图 6 所示，本发明实施例提供一种图像加密与校正装置，一种图像加密与校正装置，包括：

归一化模块 110，对亮度像素进行归一化处理生成第一像素亮度值；

加密模块 111，基于加密密钥随机生成第一随机数据，基于第一随机数据与第一像素亮度值生成加密后的第二像素亮度值；

伽马校正模块 112，基于第一伽马校正参数对第二像素亮度值进行伽马校正得到第三像素亮度值；

相应的，所述基于第一随机数据与第一像素亮度值的生成加密后的第二像素亮度值，包括：对第一随机数据与第一像素亮度值的乘积进行对数运算，从而生成加密后的第二像素亮度值。

相应的，所述第一随机数据为随机正浮点数。

相应的，基于第一伽马校正参数对第二像素亮度值进行伽马校正，包括：通过第一伽马校正参数与第二像素亮度值相乘，获得校正后的亮度值。

实施例四

如图 7 所示，本发明实施例提供一种图像解密装置，相应的，包括：

第一获取模块 210，获得第一随机数据、第一伽马校正参数以及第三像素亮度值；

还原模块 211，基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值；

去归一化模块 212，对第一像素亮度值进行去归一化处理，生成伽马校正后的亮度值。

相应的，基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值，包括：基于公式 $\bar{y}=\begin{cases}2^{(z-\log_2 n^{\gamma})} & if\ z \neq -\gamma * \varepsilon \\ 0 & otherwise\end{cases}$ 进行还原出第一像素亮度值；

其中，γ为第一伽马校正参数，n 为第一随机数据，z 为第三像素亮度值。

相应的，所述第一随机数据为随机正浮点数。

实施例五

本发明实施例提供一种图像加密与校正系统，包括：所述系统包括由上述实施例三所述的图像加密与校正装置以及实施例四所述的图像解密装置。

本发明，在基于上述实施例方案，从而对于用户端加密、上传后的图像，在不进行解密的情况下执行伽马校正处理，一方面大大提高了使得图像质量；另一方面，由于基于解密图像数据进行伽马校正处理，保护了用户端图像的私密性，保证用户数据安全；此外，采用了对数加密方法，大大降低了相对于传统复杂函数进行图像校正的方案，大大降低了的计算量。

本领域普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机 可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包 含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器和 光学存储器等）上实施的计算机程序产品的形式。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及 其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求 书

1、一种图像加密与校正方法，其特征在于，包括：

对亮度像素进行归一化处理生成第一像素亮度值；

基于加密密钥随机生成第一随机数据，基于第一随机数据与第一像素亮度值生成加密后的第二像素亮度值；

基于第一伽马校正参数对第二像素亮度值进行伽马校正得到第三像素亮度值；所述基于第一随机数据与第一像素亮度值的生成加密后的第二像素亮度值，包括：对第一随机数据与第一像素亮度值的乘积进行对数运算，从而生成加密后的第二像素亮度值。

2、如权利要求 1 所述的方法，其特征在于，所述第一随机数据为随机正浮点数。

3、如权利要求 1 所述的方法，其特征在于，基于第一伽马校正参数对第二像素亮度值进行伽马校正，包括：

通过第一伽马校正参数与第二像素亮度值相乘，获得校正后的亮度值。

4、一种图像解密方法，其特征在于，包括：获得第一随机数据、第一伽马校正参数以及第三像素亮度值；

基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值；

对第一像素亮度值进行去归一化处理，生成伽马校正后的亮度值。

5、如权利要求 1 所述的方法，其特征在于，基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值，包括：基于公式 $\bar{y}=\begin{cases}2^{(z-\log_2 n^{\gamma})} & if\ z \neq -\gamma * \varepsilon \\ 0 & otherwise\end{cases}$ 进行还原出第一像素亮度值；

其中，γ为第一伽马校正参数，n为第一随机数据，z为第三像素亮度值。

6、如权利要求 4 或 5 所述的方法，其特征在于，所述第一随机数据为随机正浮点数。

7、一种图像加密与校正装置，其特征在于，包括：

归一化模块，对亮度像素进行归一化处理生成第一像素亮度值；

加密模块，基于加密密钥随机生成第一随机数据，基于第一随机数据与第一像素亮度值生成加密后的第二像素亮度值；

伽马校正模块，基于第一伽马校正参数对第二像素亮度值进行伽马校正得到

第三像素亮度值；

所述基于第一随机数据与第一像素亮度值的生成加密后的第二像素亮度值，包括：对第一随机数据与第一像素亮度值的乘积进行对数运算，从而生成加密后的第二像素亮度值。

8、如权利要求 7 所述的图像加密与校正装置，其特征在于，所述第一随机数据为随机正浮点数。

9、如权利要求 7 所述的图像加密与校正装置，其特征在于，基于第一伽马校正参数对第二像素亮度值进行伽马校正，包括：

通过第一伽马校正参数与第二像素亮度值相乘，获得校正后的亮度值。

10、一种图像解密装置，其特征在于，包括：

第一获取模块，获得第一随机数据、第一伽马校正参数以及第三像素亮度值；

还原模块，基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值；

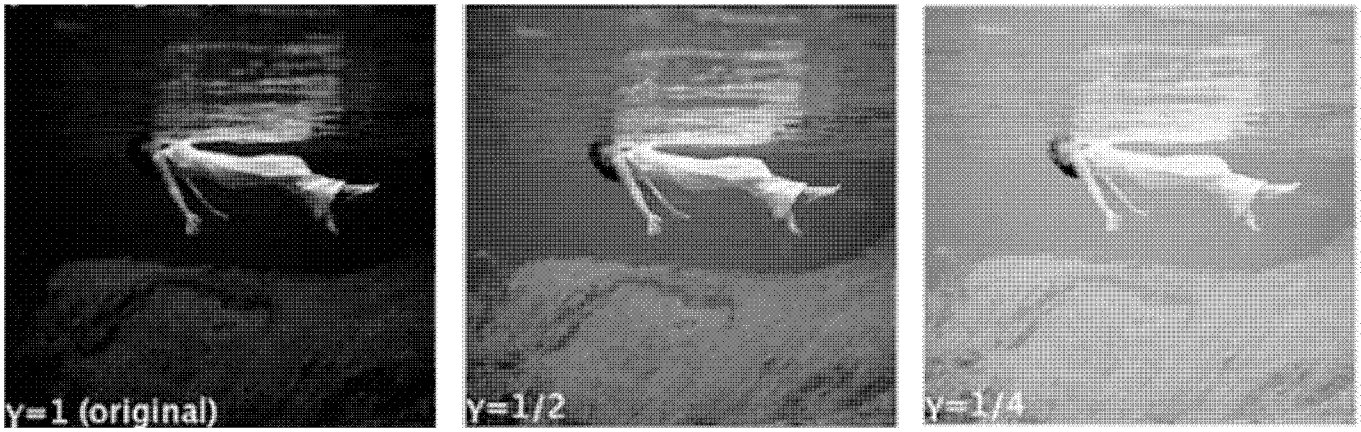
去归一化模块，对第一像素亮度值进行去归一化处理，生成伽马校正后的亮度值。

11、如权利要求 10 所述的图像解密装置，其特征在于，基于第一随机数据、第一伽马校正参数以及第三像素亮度值还原出第一像素亮度值，包括：基于公式 $\bar{y}=\begin{cases}2^{(z-\log_2 n^{\gamma})} & if\ z \neq -\gamma * \varepsilon \\ 0 & otherwise\end{cases}$ 进行还原出第一像素亮度值；

其中，γ为第一伽马校正参数，n 为第一随机数据，z 为第三像素亮度值。6、

12. 如权利要求 10 或 11 所述的图像解密装置，其特征在于，所述第一随机数据为随机正浮点数。

13、一种图像加密与校正系统，其特征在于，包括：所述系统包括由权利要求7-9任一项所述的图像加密与校正装置以及权利要求10-12任一项所述的图像解密装置。


γ=1 (original)
γ=1/2
γ=1/4

（a） （b） （c）

图 1

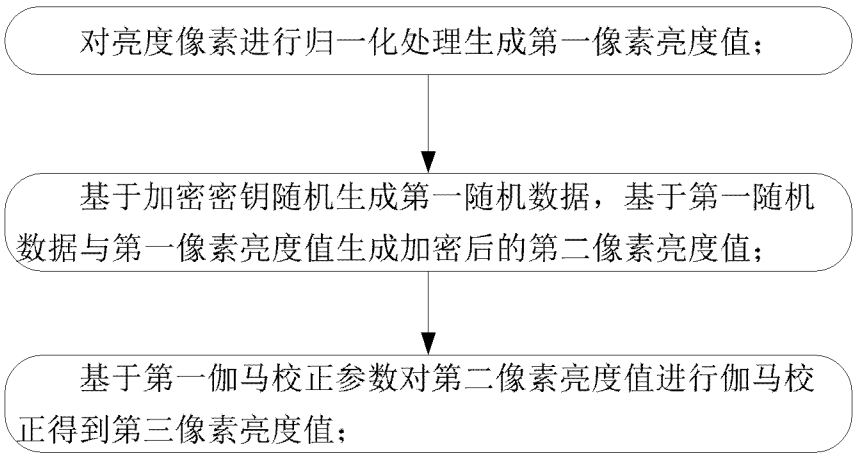

对亮度像素进行归一化处理生成第一像素亮度值；
基于加密密钥随机生成第一随机数据，基于第一随机数据与第一像素亮度值生成加密后的第二像素亮度值；
基于第一伽马校正参数对第二像素亮度值进行伽马校正得到第三像素亮度值；

图 2

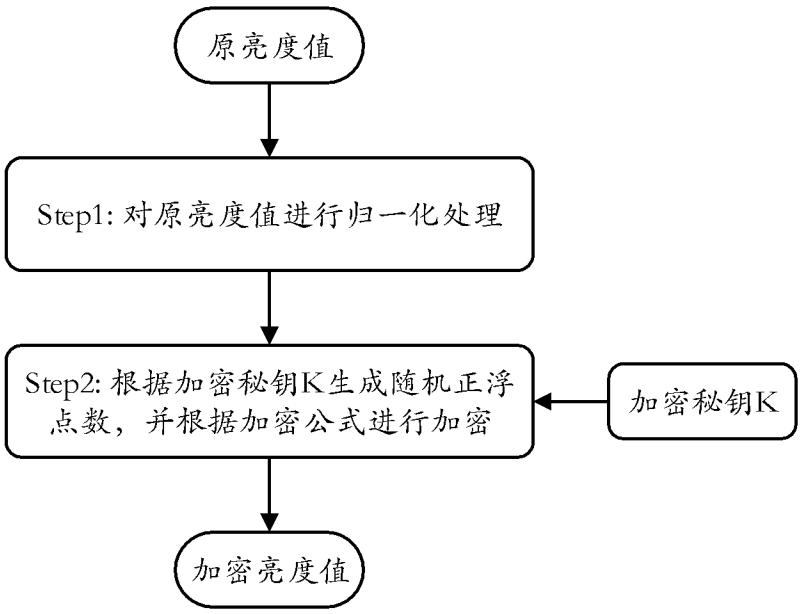

原亮度值
Step1: 对原亮度值进行归一化处理
Step2: 根据加密秘钥K生成随机正浮点数，并根据加密公式进行加密
加密秘钥K
加密亮度值

图 3

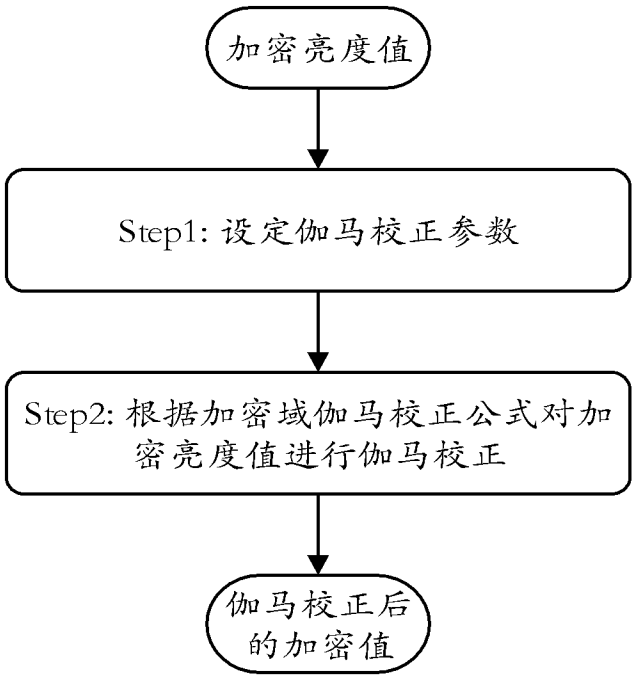

加密亮度值
Step1: 设定伽马校正参数
Step2: 根据加密域伽马校正公式对加密亮度值进行伽马校正
伽马校正后的加密值

图 4

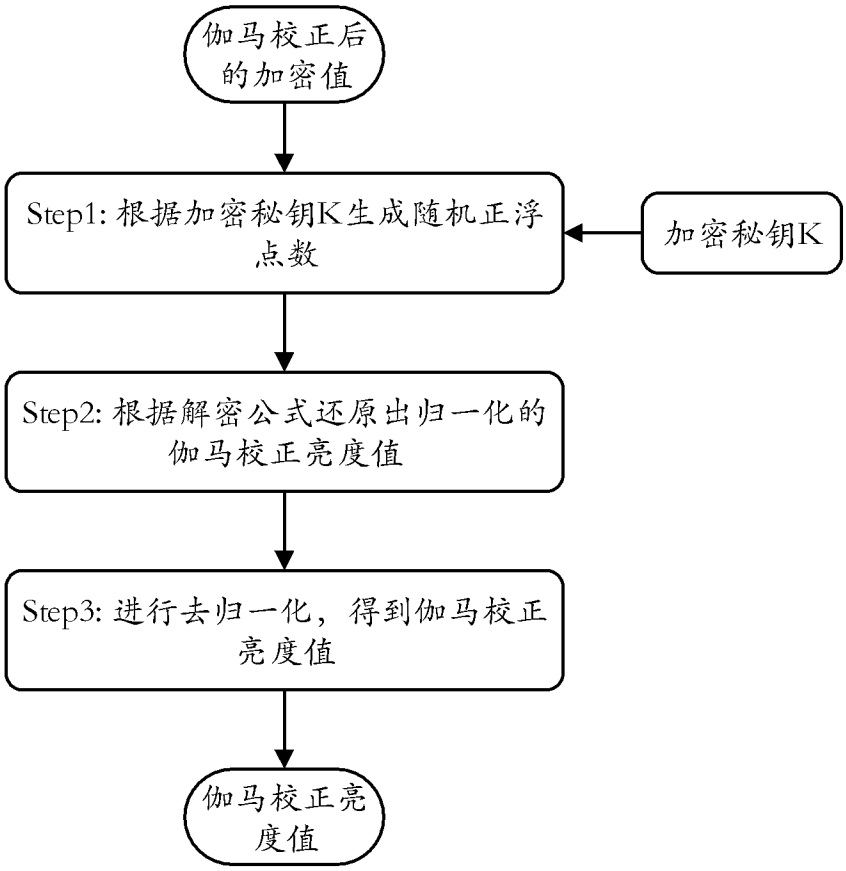

伽马校正后的加密值
Step1: 根据加密秘钥K生成随机正浮点数
加密秘钥K
Step2: 根据解密公式还原出归一化的伽马校正亮度值
Step3: 进行去归一化，得到伽马校正亮度值
伽马校正亮度值

图 5


归一化模块110
加密模块111
伽马校正模块112
图像加密与校正装置

图 6



图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/121557

A. CLASSIFICATION OF SUBJECT MATTER

H04N 1/32(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)

H04N

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)

CNPAT; CNKI; WPI; EPODOC; IEEE: 深圳先进技术研究院, 杨建权, 黄倩, 张玉兰, 常杰, 朱国普, 加密, 解密, 私密, 隐私, 密钥, 钥匙, 伽马, 伽玛, 对数, 指数, 乘法, 乘积, encrypt+, decrypt+, privacy, key, gamma, γ, log, logarithm, exponent, multiply+, product

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105830134 A (LIGHTRON FIBER-OPTIC DEVICES, INC. et al.) 03 August 2016 (2016-08-03) description, paragraphs 0063-0081	4, 6, 10, 12
A	CN 105814874 A (LIGHTRON FIBER-OPTIC DEVICES, INC. et al.) 27 July 2016 (2016-07-27) entire document	1-13
A	CN 105900421 A (TRUEPOSITION, INC.) 24 August 2016 (2016-08-24) entire document	1-13
A	CN 1450495 A (CANON K.K.) 22 October 2003 (2003-10-22) entire document	1-13
A	US 2016000301 A1 (XENOCOR, INC.) 07 January 2016 (2016-01-07) entire document	1-13

☐ 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	Date of mailing of the international search report
25 February 2020	**02 March 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/121557

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 105830134 A	03 August 2016	US 9883215 B2	30 January 2018
		KR 101819700 B1	17 January 2018
		KR 20160083113 A	11 July 2016
		CN 105830134 B	19 November 2019
		JP 6116059 B2	19 April 2017
		JP 2015115921 A	22 June 2015
		WO 2015093254 A1	25 June 2015
		US 2016330492 A1	10 November 2016
CN 105814874 A	27 July 2016	CN 105814874 B	15 March 2019
		US 2016316169 A1	27 October 2016
		KR 101807230 B1	08 December 2017
		KR 20160082704 A	08 July 2016
		WO 2015087711 A1	18 June 2015
		JP 2015114812 A	22 June 2015
		US 9762849 B2	12 September 2017
		JP 6155182 B2	28 June 2017
CN 105900421 A	24 August 2016	RU 2018112722 A	01 March 2019
		KR 20190119168 A	21 October 2019
		CN 109922344 A	21 June 2019
		JP 2018129824 A	16 August 2018
		RU 2018112722 A3	01 March 2019
		AU 2018204462 A1	12 July 2018
		AU 2015204927 A1	30 June 2016
		KR 101953286 B1	28 February 2019
		CN 109889843 A	14 June 2019
		KR 20190020848 A	04 March 2019
		EP 3092800 A1	16 November 2016
		AU 2018204462 B2	05 December 2019
		WO 2015105790 A1	16 July 2015
		CN 109889845 A	14 June 2019
		AU 2015204927 B2	22 March 2018
		RU 2688262 C2	21 May 2019
		JP 2017508342 A	23 March 2017
		CN 105900421 B	26 April 2019
		AP 201609278 D0	30 June 2016
		RU 2016132305 A	16 February 2018
		JP 6306193 B2	04 April 2018
		US 2016353123 A1	01 December 2016
		US 10440379 B2	08 October 2019
		KR 20160094441 A	09 August 2016
		RU 2653249 C2	07 May 2018
		AP 201609278 A0	30 June 2016
		CN 109889844 A	14 June 2019
		KR 102033882 B1	17 October 2019
CN 1450495 A	22 October 2003	EP 1349370 A3	07 June 2006
		EP 1349370 A2	01 October 2003
		CN 1249982 C	05 April 2006
		EP 1349370 B1	13 August 2014
		US 2007127771 A1	07 June 2007
		US 2003210803 A1	13 November 2003

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/121557

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
		US 7536026 B2	19 May 2009
US 2016000301 A1	07 January 2016	WO 2016004392 A1	07 January 2016
		MX 2017000054 A	30 June 2017
		CN 106817890 A	09 June 2017
		EP 3164047 A1	10 May 2017
		JP 2017528177 A	28 September 2017
		KR 20170024051 A	06 March 2017

国际检索报告

国际申请号
PCT/CN2019/121557

A. 主题的分类

H04N 1/32(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)

H04N

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））

CNPAT;CNKI;WPI;EPODOC;IEEE：深圳先进技术研究院，杨建权，黄倩，张玉兰，常杰，朱国普，加密，解密，私密，隐私，密钥，钥匙，伽马，伽玛，对数，指数，乘法，乘积，encrypt+，decrypt+，privacy，key，gamma，γ，log，logarithm，exponent，multiply+，product

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
X	CN 105830134 A (来特荣国际有限公司等) 2016年 8月 3日 (2016-08-03) 说明书第0063-0081段	4，6，10，12
A	CN 105814874 A (来特荣国际有限公司等) 2016年 7月 27日 (2016-07-27) 全文	1-13
A	CN 105900421 A (杜比实验室特许公司) 2016年 8月 24日 (2016-08-24) 全文	1-13
A	CN 1450495 A (佳能株式会社) 2003年 10月 22日 (2003-10-22) 全文	1-13
A	US 2016000301 A1 (XENOCOR, INC.) 2016年 1月 7日 (2016-01-07) 全文	1-13

☐ 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	国际检索报告邮寄日期
2020年 2月 25日	2020年 3月 2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 传真号 (86-10)62019451	受权官员 王兴 电话号码 86-(10)-53961701

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/121557

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	105830134	A	2016年 8月 3日	US	9883215	B2	2018年 1月 30日
				KR	101819700	B1	2018年 1月 17日
				KR	20160083113	A	2016年 7月 11日
				CN	105830134	B	2019年 11月 19日
				JP	6116059	B2	2017年 4月 19日
				JP	2015115921	A	2015年 6月 22日
				WO	2015093254	A1	2015年 6月 25日
				US	2016330492	A1	2016年 11月 10日
CN	105814874	A	2016年 7月 27日	CN	105814874	B	2019年 3月 15日
				US	2016316169	A1	2016年 10月 27日
				KR	101807230	B1	2017年 12月 8日
				KR	20160082704	A	2016年 7月 8日
				WO	2015087711	A1	2015年 6月 18日
				JP	2015114812	A	2015年 6月 22日
				US	9762849	B2	2017年 9月 12日
				JP	6155182	B2	2017年 6月 28日
CN	105900421	A	2016年 8月 24日	RU	2018112722	A	2019年 3月 1日
				KR	20190119168	A	2019年 10月 21日
				CN	109922344	A	2019年 6月 21日
				JP	2018129824	A	2018年 8月 16日
				RU	2018112722	A3	2019年 3月 1日
				AU	2018204462	A1	2018年 7月 12日
				AU	2015204927	A1	2016年 6月 30日
				KR	101953286	B1	2019年 2月 28日
				CN	109889843	A	2019年 6月 14日
				KR	20190020848	A	2019年 3月 4日
				EP	3092800	A1	2016年 11月 16日
				AU	2018204462	B2	2019年 12月 5日
				WO	2015105790	A1	2015年 7月 16日
				CN	109889845	A	2019年 6月 14日
				AU	2015204927	B2	2018年 3月 22日
				RU	2688262	C2	2019年 5月 21日
				JP	2017508342	A	2017年 3月 23日
				CN	105900421	B	2019年 4月 26日
				AP	201609278	D0	2016年 6月 30日
				RU	2016132305	A	2018年 2月 16日
				JP	6306193	B2	2018年 4月 4日
				US	2016353123	A1	2016年 12月 1日
				US	10440379	B2	2019年 10月 8日
				KR	20160094441	A	2016年 8月 9日
				RU	2653249	C2	2018年 5月 7日
				AP	201609278	A0	2016年 6月 30日
				CN	109889844	A	2019年 6月 14日
				KR	102033882	B1	2019年 10月 17日
CN	1450495	A	2003年 10月 22日	EP	1349370	A3	2006年 6月 7日
				EP	1349370	A2	2003年 10月 1日
				CN	1249982	C	2006年 4月 5日
				EP	1349370	B1	2014年 8月 13日
				US	2007127771	A1	2007年 6月 7日
				US	2003210803	A1	2003年 11月 13日

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/121557

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)
		US	7536026	B2	2009年 5月 19日
US 2016000301 A1	2016年 1月 7日	WO	2016004392	A1	2016年 1月 7日
		MX	2017000054	A	2017年 6月 30日
		CN	106817890	A	2017年 6月 9日
		EP	3164047	A1	2017年 5月 10日
		JP	2017528177	A	2017年 9月 28日
		KR	20170024051	A	2017年 3月 6日