一种新的彩色图像信息融容密码技术*)

米 佳
(辽宁警官高等专科学校公安信息系 大连 116036)

摘 要 本文从色度学的角度提出了一种全新的密码技术—彩色图像信息融容密码技术,即根据色度学理论,将待传输或存储的彩色图像原文和用于加密或解密的彩色图像密钥在RGB颜色空间和XYZ颜色空间中进行线性和非线性的定量变换,使颜色信息得以融容,形成难以辨认和破解的密码图,从而实现对文本、图像的传递。
关键词 彩色图像信息,融容密码,加密技术

A New Encryption Technique for Color Image Information Based on Melting Encryption

MI Jia
(Police Information Department, Liaoning Police Academy, Dalian 116036)

Abstract A new encryption technique for color image information is proposed based on melting encryption in light of color science. Linear and nonlinear transformation of quantity are applied to the two color images in the RGB and XYZ color space, and these two color images are individually the origin color image used for transporting or storing and the color image used for encryption or decryption. Then color image information is melted to encryption map, which can't be identified and decryption easily. So the texts and images can be transported secretly and securely.
Keywords Color image information, Melting encryption, Encryption technique

1 引言

密码技术是利用密码学的原理和方法对传输的数据进行保护的方法,它以数学计算为基础[1]。近年来,我国政府高度重视密码技术的研究,强调要加强建立和完善以密码技术为基础的信息保护和网络信任体系,大力发展拥有自主知识产权的密码技术,研究开发多算法、多应用、多协议的密码平台,满足电子商务、电子政务发展的需要,解决密码设备的互通、兼容问题。如今,许多数学家、计算机专家、应用领域专家都在研究和发展密码技术。

图像信息形象、生动,已被人类广为利用,成为人类表达信息的重要手段之一。同时为了确保图像数据在传输过程中的安全性,就需要可靠的图像数据加密技术。齐东旭等人[3,4]提出了基于矩阵变换和像素变换的加密技术,但由于基于矩阵变换加密技术的攻击对于现代计算机来说时间是很短的,基于像素变换加密技术是一线性变换,因而其保密性都不高。文[4,5]提出了基于密码分割和密码共享的图像加密技术。基于密码分割的图像加密技术存在这样一个问题:如果秘密的一部分丢失了而作为仲裁人的Trent又不在,就等于把秘密丢失了,而且这种一次一密类型的加密体制是有任何计算能力和资源的个人和部门都无法恢复秘密的;而基于密码共享的图像加密技术缺点是图像数据量发生膨胀,这在图像数据本来就很庞大的情况下给图像的网络传输带来了严重的困难,限制了这种加密算法在实际中的应用,而且对于采用这种门限方案的算法其恢复出的图像的对比度会有所下降。基于现代密码体制的加密技术是把待传输的图像看作明文,通过各种加密算法,如DES,RSA等,在密钥的控制下,达到图像数据的保密通信。这种加密机制的设计思想是加密算法可以公开,通信的保密性完全依赖于密钥的保密性(即满足Kerckhoffs假设)[2]。本文正是在基于现代密码体制的加密技术的基础上,从色度学的角度提出了一种全新的密码技术——彩色图像信息融容密码技术,即根据色度学理论,将待传输或存储的彩色图像原文和用于加密或解密的彩色图像密钥在RGB颜色空间和XYZ颜色空间中进行线性和非线性的定量变换,使颜色信息得以融容,形成难以辨认和破解的密码图,对文本、图像的传递实现保密。主要有以下两个优点:1.本文将乱码图像作为密钥,可以由信息传递双方约定随时生成,也可以建立彩色图像密钥库,其灵活性确保了传输的安全性;2.本文算法同时使用了线性和非线性的定量变换,因而具有很高的保密性。本文的实验证明了本文的安全性和保密性。

本文第2节在引入两个关键技术的基础上,提出了彩色图像信息融容密码技术的算法思想及其步骤;第3节给出了该技术的实现并展示了实验效果;最后是结论。

2 彩色图像信息融容密码技术的算法

本节在引入两个关键技术—密码算法与密钥、色度学理论—的基础上,提出了彩色图像信息融容密码技术的算法思想及其步骤。

2.1 密码算法与密钥

密码技术研究与应用中,关键是密码算法和密钥。

密码算法也叫密码,是用于加密和解密的数学函数。通常情况下有两个相关的函数,一个用作加密,一个用作解密。

为了保证信息传输和处理过程中的机密性,现代密码学利用密钥解决算法受限的问题。假设密钥用K表示,K可以是很多数值里的任意值。密钥K的可能取值的范围叫做密钥空间。加密和解密运算都使用这个密钥(即运算都依赖于密钥,并用K作为下标表示),这样加密函数E和解密函数D现在变成:

$$E_k(M)=C$$

*)基金项目:大连市科技局科技计划项目(2005E21SF147)。米 佳 副教授,硕士。

$D_k(C)=M$

其中 M 为明文，C 为密文。或者写成：

$D_k(E_k(M))=M$

有些算法使用不同的加密密钥和解密密钥，也就是说，加密密钥 K_1 和解密密钥 K_2 不同，此时，

$E_{k1}(M)=C$

$D_{k2}(C)=M$

$D_{k2}(E_{k1}(M))=M$

为了能够获得安全的密码算法和密钥，彩色图像信息融容密码术则是根据色度学理论，将待传输或存储的彩色图像原文和用于加密或解密的彩色图像密钥在 RGB 颜色空间和 XYZ 颜色空间中进行线性和非线性的定量变换，使颜色信息得以融容，形成外观无序内在有序的颜色组合，窃密者尽可观之，不可知之。

2.2 色度学原理的应用

在计算机系统中，彩色图像中每一像素的颜色三刺激值通常用标准的红绿兰 RGB 值表示。R 代表颜色的红基色分量，G 代表绿基色分量，B 代表兰基色分量，通常称之为 RGB 颜色空间。计算机 RGB 三个通道中的每一通道通常分为 2^8 即 256 个等级，因此，三个通道可组合成 2^{24} 即 16.7 兆种颜色。每组 RGB 值，在颜色空间中代表一个颜色；反之，颜色空间中的任何一个颜色，会有一组确定的 RGB 值与其对应。计算机系统中的颜色 RGB 值均为正值，不包括那些含有负值分量的颜色。

由于 RGB 颜色空间是与设备有关的颜色空间，有很多的不足，因此，国际照明委员会 CIE 建立了 CIE 1931XYZ 颜色空间，颜色用三刺激值 XYZ 表示。每一颜色有确定的 XYZ 值，如图 1 所示。

图 1 CIE 1931XYZ 颜色立体空间色度图

RGB 颜色空间和 XYZ 颜色空间可以用下式进行彼此之间三刺激值的转换：

$$\begin{aligned} X&=a_{11}R+a_{12}G+a_{13}B \\ Y&=a_{21}R+a_{22}G+a_{23}B \\ Z&=a_{31}R+a_{32}G+a_{33}B \end{aligned} \tag{1}$$

当然，上式可用矩阵形式表示，并可用逆矩阵形式表示 XYZ 向 RGB 的转换。其中矩阵的九个系数可以根据色度学知进行标定。

2.3 彩色图像信息融容密码技术算法思想及步骤

目前已经有很多文献提出了针对数字图像的加密方法。图像加密算法主要是在空间域和频率域进行的。空间域算法的优点是能够充分利用图像数据流的点阵特征使算法更直观，实现比较简单，且加密过程中不会引入额外的图像畸变[9]。但大多存在一个缺陷：密钥图像的单一性。本文正是针对这一缺陷提出了一个全新的密码技术——彩色图像信息融容密码技术，该算法将乱码图像作为密钥，可以由信息传递双方约定随时生成，也可以建立彩色图像密钥库，具有很强的灵活性；它同时使用了线性变换和非线性变换，因而具有很强的保密性。

本文技术加密算法思想可概述如下：明文彩色图像中某个像素的刺激值为 $R_iG_iB_i$ 和 $X_iY_iZ_i$，密钥彩色图像对应像素的刺激值为 $R_jG_jB_j$ 和 $X_jY_jZ_j$。根据色度学理论，在 CIE 色立体中，选择一种数学函数或数学处理方法，确定色度点 $X_iY_iZ_i$ 和 $X_jY_jZ_j$ 转换对应的色度点 $X_mY_mZ_m$，并根据(1)式的逆矩阵确定出密文该像素的 $R_mG_mB_m$。对每一像素作不同的数学变换，获得整个彩色图像明文的加密密文彩色图像。

对图像中某个像素，具体算法步骤如下：

Step 1：将明文彩色图像中某个像素的刺激值 $R_iG_iB_i$ 利用式(1)转化成 $X_iY_iZ_i$；

Step 2：将密钥彩色图像对应像素的刺激值 $R_jG_jB_j$ 也利用式(1)转化成 $X_iY_iZ_i$；

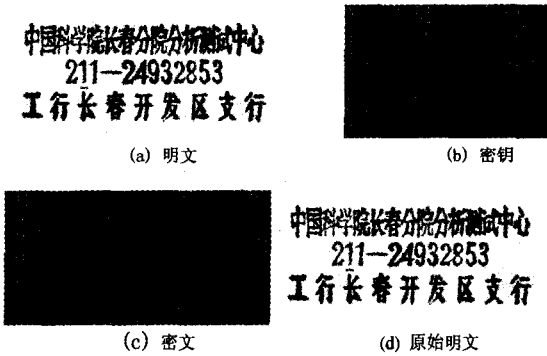
Step 3：在 CIE 色立体中，选择一种数学函数或数学处理方法，确定色度点 $X_iY_iZ_i$ 和 $X_jY_jZ_j$ 转换对应的色度点 $X_mY_mZ_m$；

Step 4：并根据(1)式的逆矩阵确定出密文该像素的 $R_mG_mB_m$。

解密是加密的逆处理，也就是说，在色立体中，色度点 $X_iY_iZ_i$ 和 $X_jY_jZ_j$ 与 $X_mY_mZ_m$ 是确定的一组，利用加密时使用的数学函数的逆变换，必然得到唯一的解 $X_iY_iZ_i$，从而得到原始明文 $R_iG_iB_i$。

3 算法实现及实验结果

要想实现上述思想，建立密钥彩色图像和编写了计算机加密解密软件是关键。彩色图像的图像格式有很多种，BMP 格式的彩色图像质量较好、图像采集存储相对简单。所以，基于上述原理，在研究中我们重点对 BMP 格式的彩色图像信息融容加密技术进行了研究，利用 C 语言编制了彩色图像信息融容密码术计算机加密解密程序，并由秘密明文发送方和接受方分别持有加密程序和解密程序。这些程序已经经过编译，形成可执行程序，具有一定的反编译能力，在编制程序时已经考虑到，即使当窃密方破译了加解密程序，也只能了解彩色图像信息融容密码术的算法，成他所用，但对我们的信息安全传输和存储无任何妨碍。



(a) 明文　(b) 密钥　(c) 密文　(d) 原始明文

图 2 加密和解密流程举例

其他格式的图像可以方便地通过已有的图像处理软件进行相互转换，得以加密和解密，实现信息的安全传输和存储。

彩色图像信息融容密码术包括对称算法和非对称算法，并形成隐型加密和显型加密，因此，发送方和接受方要事先根

据算法和加密类型做出约定。

以隐型对称算法加密为例，其流程如图 2 所示：分别为明文、密钥、密文和原始明文。

密钥是乱码彩色图像，密码算法又不被人知晓，密文是不会被他人破解。实现了信息的安全传输或存储。

至于彩色图像密钥，可以由信息传递双方约定随时生成，也可以建立彩色图像密钥库。私钥彩色图像也是由编制的计算机软件生成，每个私钥均可由不同的运算形式产生，因此，密钥的灵活性更确保了信息传输的安全型。公钥可以使用任何彩色图像，甚至包括从网络上下载的彩色图像，只要下载的图像相同即可。

对于对称算法，加密密钥和解密密钥相同，因此，需要使用相同的密钥生成程序形成加解密密钥。只要密钥不被他人窃取，密文不会被破译的，信息安全能够得到保证。

至于非对称算法，发送方和接受方使用的是公钥，加密和解密密钥是公开的。虽然，彩色图像密钥被世人所知，但是，彩色图像信息融容密码术的算法仍旧能够保证信息的安全。因为，本密码术可以做到，即使窃密方搞到彩色图像密钥，但不知算法，仍旧不能破译密文。这也就是为什么在一个集团内，例如某某公司，大家使用公开的彩色图像密钥库，两人之间的密文传送，不会被集团内的第三人所破解。否则，密码技术也不能称之为安全可靠。

对于隐型加密，使用的彩色图像密钥是乱码图像。虽然看上去是乱码图，但是每个像素的 RGB 颜色色度值是确定的，是由发送方和接受方事先使用密钥生成程序形成，或由彩色图像密钥库事先选择约定。图 3 是两个完全不同的彩色图像密钥。

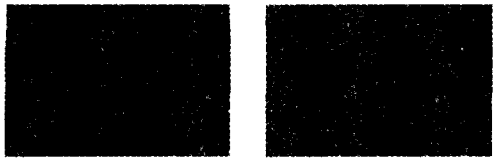


图 3　两个完全不同的彩色图像密钥

至于显型加密，彩色图像密钥是视觉上看起来很普通的彩图，例如生活照片、风景画、网上下载的图片等等均可，目的就是不被人怀疑。因为显型加密有两类，一类是仅仅使用视觉主观隐藏，解密后的还原图像不被人主观感知与原始图像的些许差异；另一类是客观隐藏，解密后的还原图像要与原始图像相同，可以满足计算机的判读识别。当然，客观隐藏技术要比主观隐藏技术复杂一些，需要把主观隐藏方法中的不足弥补上去，需要两倍的处力量。但是，主观隐藏方法相对简单，且能满足视觉上的识别。

为了提高本密码术的保密强度，在编制的加密解密软件中，增加一些选项，例如彩色图像密钥像素的选取间隔，是逐点顺序选取还是隔几点非规则选取；再如彩色图像密钥的大小，是与彩色图像密文大小相同，还是与密文图像大小不等，或大或小。这些变量可以使窃密者更难下手破译密码原文。

结论　本文根据色度学理论提出一种全新的密码技术—彩色图像信息融容密码技术。由于该技术密钥灵活，且对原图像和密钥图像同时进行了线性和非线性变换，因此具有很高的安全性和保密性。经过实验和检验，算法理论简单，保密性强，加密速度快，本密码技术产品的成本相对较低，只需简单的软件即可实现加密和解密，不需要昂贵的硬件支持，一旦形成产品，可在信息安全传输存储等方面发挥巨大作用。

参 考 文 献

1　王宇洁，许占文，郑守春. 密码技术综述. 沈阳工业大学学报，2000，22(5)：406～409
2　李昌刚，韩正之，张浩然. 图像加密技术综述. 计算机研究与发展，2002，39(10)：1317～1324
3　齐东旭. 矩阵变换及其在图像信息隐藏中的应用. 北方工业大学学报，1999，11(1)：24～28
4　丁玮，齐东旭. 数字图像变换及信息隐藏与伪装技术. 计算机学报，1998，21(9)：838～843
5　Schneier B. 应用密码学——协议、算法与 C 源程序. 北京：机械工业出版社，2000
6　Shamir A. How to share a secret. Communications of ACM，1979，22(11)：612～613
7　张文华，陈雅颂，穆国旺. 基于素数的图像置乱技术. 河北工业大学学报，2006，35(4)：1～4
8　王英，郑德玲，王振龙. 空域彩色图像混沌加密算法. 计算机辅助设计与图形学学报，2006，18(6)：876～880
9　李谦. 基于混沌序列和 DES 的彩色图像加密算法的研究. 计算机工程与设计，2006，27(6)：999～1004
10　斯廷森著. 密码学原理与应用(第二版). 冯登国译. 电子工业出版社，2003，3
11　Baker M P. Computer Graphics：C version，Second Edition. Donald Hearn，2003，4
12　陆系群，陈纯. 图像处理原理技术与算法. 浙江大学出版社，2001，8
13　汤顺青. 色度学. 北京理工大学出版社，2002
14　Castlemun K R. Digital Image Processing(影印版). 清华大学出版社，1998

(上接第 230 页)

结论和下一步工作　由于利用肤色信息进行肤色区域检测具有较低的计算量，能够和大多数背景区域区分开，可以有效地减小人脸检测、定位的搜索空间，因此肤色常被用于彩色图像中的人脸候选区域检测。但是由于肤色特征对光照变化很敏感，因此，基于肤色的人脸检测方法在实际应用前必须排除光照的影响。

本文提出的人脸区域初检测方法，考虑了以下问题：在 RGB 颜色空间对彩色图像进行色彩平衡校正；选择亮度和色度分离的新颜色空间 YCgCr，建立了肤色模型，最后对经过形态学开运算操作去噪后的二值图像引入预处理技术，进行非人脸肤色区域去除。实验结果表明，文中的方法具有较好的人脸初定位效果。

我们下一步的工作就是在人脸区域初检结果的基础上，采用模板脸匹配技术或 SVM 等统计学习的方法，进行人脸区域验证并定位。

参 考 文 献

1　Yang M H，Kriegman D J，Ahuja N. Detecting faces in images：A survey. IEEE transactions on Pattern analysis and machine intelligence，2002，24(1)：34～58
2　Hsu R L，Abdel-Mottaleb M，Jain A K. Face detection in color images. IEEE transactions on pattem analysis and machine intelligence，2002，24：696～706
3　Chiang J. Gray World Assumption. http://ise. stanford. edu/class/psych221/projects/99/ jchiang/intro2. html
4　Terrillon J C，Shirazi M N，Fukamachi H，et al. Comparative performance of different skin chrominance models and chrominance spaces for the automatic detection of human faces in color images. In：Proceedings of Fourth IEEE International Conference on Automatic Face and Gesture Recognition，2000. 54～63
5　Phung S L，Bouzerdoum A，Chai D. A novel skin color model in YCbCr color space and its application to human face detection. In：Proceedings of International Conference on Image Processing，2002，1：289～292
6　de Dios J J，Garcia N. face detection based on a new color space YCgCr. In：Proceedings of International Conference on Image Processing，2003，3：909～912
7　艾海舟，武勃，等译. 图像处理、分析与机器视觉(第二版)[M]. 北京：人民邮电出版社，2003