数字图像加密综述

文昌辞[1] 王 沁[1] 苗晓宁[2] 刘向宏[2] 彭阳翔[2]
(北京科技大学计算机科学与技术系 北京 100083)[1] (空军装备部 北京 100009)[2]

摘 要 针对数字图像的特点,分析了传统加密算法不适用的原因,陈述了数字图像加密的现状,对基于空间域的像素置乱、基于混沌的加密、基于变换域的加密、基于秘密分割与秘密共享的加密、基于神经网络和元胞自动机的加密以及基于盲源分离的加密进行了详细描述,并对它们的特点进行了分析比较。最后,举例分析了大量典型的加密算法,指出了它们的不足,并探讨了进一步的研究方向。

关键词 图像加密,置乱,混沌,空间域,变换域
中图法分类号 TP391 **文献标识码** A

Digital Image Encryption: A Survey

WEN Chang-ci[1] WANG Qin[1] MIAO Xiao-ning[2] LIU Xiang-hong[2] PENG Yang-xiang[2]
(Department of Computer Science and Technology, University of Science and Technology Beijing, Beijing 100083, China)[1]
(Air Force Equipment Department, Beijing 100009, China)[2]

Abstract According to the feature of digital image, the reason why traditional cipher algorithms are not applicable was analyzed, and the development of digital image encryption was surveyed. Some techniques, such as pixel permutation in space domain, encryption based on chaos, encryption in transform domain, image secret segmentation and sharing, encryption based on neutral network and cellular automata, encryption based on blind source separation, were illustrated, and the corresponding characteristics were analyzed and compared. At last, a large number of typical encryption algorithms were analyzed in detail to expose their weakness, and the future research direction was discussed.

Keywords Image encryption, Scramble, Chaos, Space domain, Transform domain

1 引言

在诸如军事协同作战、电子政务、工业协同设计、场景监控、远程医疗与远程教育等传输系统中,需要可靠的图像加密技术。传统加密算法针对一维数据流而设计,如 DES、3-DES、IDEA、AES,没有考虑数字图像具有数据量大、空间有序、相关性强、冗余度高的特点,具有较高的计算复杂度,加密效率也不高。图像加密算法有如下几个要求:①安全性。混淆和扩散是当前设计具有计算安全性的密码的必要条件。②实时性。加密算法的使用不能给图像数据传输和存取带来过大的延迟。③数据量不发生膨胀。为了不给存储、传输带来更大的负担,加密处理不能使密文数据量发生膨胀。如果可以,应尽量结合压缩编码进行。④数据格式不变。不加密与图像格式密切相关的数据字段,可以尽量减少明密文对的泄漏。另外,在一些应用中需要保持格式兼容。

2 数字图像加密研究现状

目前,数字图像加密算法按加密思路主要分为以下几类:基于空间域的像素置乱、基于混沌的加密、基于变换域的加密、基于秘密分割与秘密共享的加密、基于神经网络和元胞自动机的加密、基于盲源分离的加密。

2.1 基于空间域的像素置乱

置乱变换可以快速地打乱像素位置,破坏图像中原有的空间有序性和局部相关性,把图像变得杂乱无章、无法识别,使图像呈现一种类似噪声的形式。为了保证加密之后还能正确恢复,置乱变换必须为一一映射。目前的置乱方法有:Arnold 变换及其扩展变换(如猫映射、广义猫映射[1]、二维双尺度矩形映射、仿射变换、n 维广义 Arnold 变换)、Baker 映射、幻方变换、魔方变换、基于 S 盒的置乱、基于拉伸折叠思想的置乱、基于 Scan 语言的置乱、基于骑士巡游的置乱、基于随机数排序的置乱、基于像素值排序的自适应置乱、基于线映射的置乱、基于队列的置乱和基于四叉树编码的置乱等。

在上述置乱方法中,Arnold 变换及其扩展变换采用了矩阵变换的形式,它们同 Baker 映射一样都能快速地将相邻像素分散开,像素的移动具有混沌特性,而且耗费的计算量很小。基于仿射变换的置乱使得所有的像素点均可能改变了位置,而猫映射、广义猫映射、二维双尺度矩形映射没有改变(0,0)处像素的位置,这可能成为包含置乱操作在内的整个算法的

到稿日期:2012-02-03 返修日期:2012-07-05 本文受装备预研重点基金(9140A04040308DZ1002)资助。
文昌辞(1980—),男,博士生,工程师,主要研究方向为计算机系统结构、信息安全,E-mail:wenchangci@126.com;**王 沁**(1961—),女,博士,教授,博士生导师,主要研究方向为计算机系统结构、信息安全、芯片设计;**苗晓宁**(1975—),男,硕士,工程师,主要研究方向为信号处理、信息安全;**刘向宏**(1968—),男,硕士,高级工程师,主要研究方向为信号处理;**彭阳翔**(1982—),男,工程师,主要研究方向为信息安全。

安全漏洞。基于猫映射变换、幻方变换、骑士巡游的置乱对图像的长宽比例有限制，使得它们的适用范围有限。基于随机数排序的置乱先产生一个随机数序列，将该序列中各数值的大小对应设置为图像中各像素的权值，按权值大小对像素进行排序，以达到置乱的效果。基于像素值排序的自适应置乱用图像中一部分像素值的大小对应作为图像中另一部分像素的权值，按权值大小对这另一部分像素进行排序；如此交替赋以权值并进行排序，以达到置乱的效果。基于排序的置乱算法时间复杂度较高，而且为了存储对应的像素位置，可能还需要额外的存储空间，所以空间复杂度也较高。基于四叉树编码的置乱结合了无损压缩编码，它在形成四叉树之后对四叉树的内部节点和叶子节点进行置乱，以达到加密的效果。

目前已有的置乱算法大都不改变像素值，它们通过对明密文的像素直接进行比对就可能发现置乱规律，但安全性较低。同时，由于离散数字图像是有限点集，在置乱变换若干次以后图像终究会回复到初始状态，因此只要知道加密算法，按照密文空间的任意一个状态来进行迭代，都会在有限步内恢复出明文。

2.2 基于混沌的加密

混沌系统是非线性的系统，表现出非常复杂的伪随机性，符合混淆规则。它对初始条件和控制参数非常敏感，任何微小的初始偏差都会被指数式放大，符合扩散规则。同时，它又是确定性的，可由非线性系统的方程、参数和初始条件完全确定。因此，初始状态和少量参数的变化就可以产生满足密码学基本特征的混沌密码序列，将混沌理论与加密技术相结合，可以形成良好的图像加密系统。目前常用于图像加密的混沌系统有：Logistic 混沌映射、Chebychev 映射、分段线形混沌映射、Cubic 映射、标准映射、Henon 映射[2]、Lorenz 混沌映射、蔡氏混沌、Rossler 混沌系统、二维 Sinai 映射、Chen's 混沌系统等。

在基于混沌的图像加密方法中，有的利用混沌系统产生伪随机序列，进行序列密码形式的加密。有些利用混沌的遍历性，对产生的伪随机序列作处理，得到像素置乱后的位置，然后对像素位置进行置乱。有些利用一些混沌计算表达式可逆的特点，将像素值代入混沌计算式以进行像素的代换和扩散[2]。与传统加密算法相比，混沌图像加密算法密钥空间大，实现简单，加密速度快，但是，基于混沌的图像加密存在以下不足：

①计算机的有限精度可能导致混沌序列的周期比较短，随机性不好。文献[3]对一个用于图像加密的混沌系统进行了分析，发现通过对该混沌系统产生的数值进行处理后，用于流密码加密的操作数有很多个为 0；它指出用这种方法产生伪随机数来加密图像是不安全的，并列举了几个图像加密实例，从这些密图中可以不同清晰程度地看到明文中的人物。文献[4]针对大多数加密算法一次仅加密一个图像而实际中需要通过批处理来传输大量图像的情况，提出了一种结合向量量化和索引压缩的批图像加密算法；它实际上是在向量量化后将所得到的索引采用流密码形式加密。由于处理批量图像时数据量太大，因此它对产生的随机序列要求很高。在实际中，混沌系统还可能存在"平凡密钥"或"拟平凡密钥"，如果用它们作为初始值，则将无法产生可用的混沌序列。

②现有的混沌加密技术大都基于一维或二维混沌系统，容易受到相空间重构方法攻击。攻击者有可能利用现有的分析技术得到混沌系统的参数设置，从而破译算法。目前，对于混沌加密系统的分析和攻击都是针对低维的，研究高维混沌系统或者超混沌系统[5]可能寻找出演化规律更复杂、更随机的混沌加密方案。另外一种办法是尽量将多个混沌系统相复合，以避免直接暴露混沌轨道信息。

③一些混沌加密算法采用了形式比较复杂的混沌系统，速度较慢，无法实现实时的加密。而且，如果所采用的混沌系统是连续时间的混沌系统，在生成混沌序列时就需要积分运算，计算量太大。在设计算法时，应尽量使用形式简单的离散时间混沌系统。另外，应尽量避免过多的加密轮数。有些加密算法往往迭代很多轮才得出密文，降低了加密效率。

2.3 基于变换域的加密

变换域中每一个系数的改变都会导致图像空间域中所有像素值的改变，因此可以通过在变换域对系数进行处理来达到加密的效果。由于计算机精度有限，基于变换（如 DFT、DCT、DWT、FRFT[6]、FRHT[7]、FrMT[8]、MPDFrRT[9]）域的加密算法在变换与反变换时存在数据精度损失，解密后的图像与明文不会完全相同。另外，如果将从空域映射到变换域的操作仅仅作为一个加密运算步骤[6-9]，而未将其结合到压缩编码中，那么所耗费的计算量就没有得到充分利用。在不要求解密所得与明文完全一致的情况下，应优先采用结合有损压缩的加密算法。

以 JPEG、JPEG2000 有损压缩编码为例，分析可知，结合有损压缩的加密算法应在变换域系数被量化之后再进行位置置乱、代换或者扩散，即量化时依然是让代表图像细节信息的高频系数损失得多，代表图像重要信息的低频系数损失得少，尽可能保持图像的质量，并且使压缩不影响加密。

如果仅置乱量化后的系数的位置或改变系数的符号，则安全性不高。类似于分析空域像素直接加密的算法，攻击者可以通过比对明、密文图像变换域量化后的系数来找出置乱规律，从而破解加密算法。所以，基于变换域的数字图像加密也需要代换、扩散操作。

如果针对频域所有量化后的系数进行全局的置乱、代换、扩散，那么就可能极大地破坏量化后系数的大小分布规律，使得压缩效果不好。如果加密算法先在空间域进行像素的置乱，然后进行空域到变换域的变换、量化，最后加密量化后系数，那么逆向操作（即解密）之后的图像质量会受到很大影响，而且由于一开始就破坏了图像中的局部相关性和空间有序性，压缩效果也不好。

综上，为了降低加密对压缩的影响并保留较好的图像质量，在变换域系数被量化之前尽量不采用加密操作，并且在变换域系数被量化后，应采取局部置乱、代换和扩散的方法，这样才能减少加密的数据量，提高加密效率。

2.4 基于秘密分割与秘密共享的加密

秘密分割就是把消息分成许多碎片，每一个碎片本身不代表任何意义，但把这些碎片放到一起就可以重现原来的信息。该方法存在的问题是：当分割后的碎片中任一个出现问题（如丢失）时，整个信息就不能恢复出来。这种思想用于图像加密就是先把明文图像按某种算法进行分割，并把分割后的数据交给不同的接收者，需要保存数据的所有接收者共同参与，才能恢复出原始明文。

基于秘密共享的加密算法是由密钥分存的概念发展起来的，即把密钥 K 分解为 n 个子密钥 $K(i)$，并且满足任意 m 个

子密钥的结合才能恢复密钥 K，若少于 m 个则不能得到密钥 K 的任何信息。在进行图像加密时，把图像分成 n 部分，其中任意 m 部分($m \leqslant n$)可以重构原来的图像，但少于 m 部分则得不到原来图像的任何信息。秘密共享的优点在于个别子数据的泄漏不至于引起明文的泄漏，而个别子数据的损失也不至于影响明文的恢复。

基于秘密分割与秘密共享的方法在用于图像加密时，会使得密文数据量发生膨胀，给本来数据量就大的图像带来更大的存储、传输负担。文献[10]针对 JPEG 图像提出了一种秘密共享的加密算法，它将变换域量化后的系数进行分解，生成若干个与明文图像长宽尺寸相同的新图像，每个新图像单独不可识别。在得到一定数量的新图像后将它们的变换域系数相异或即可恢复出明文。该算法不仅使得密文数据量发生膨胀，而且没有将安全性寓于密钥之中，不符合 Kerckhoff 原则，所以不适合作为密码算法。

2.5 基于神经网络和元胞自动机的加密

人工神经网络是由许多简单的、高度互联的神经元构成的，它对外部输入进行动态的信息处理，其特点是并行分布处理模式。此外，神经网络还具有非线性、联想记忆的特点，因此适合于信息的加密。文献[11]利用离散 Hopfield 神经网络生成伪随机序列，与明文数字图像逐位异或得到密文，加密框图见图 1。

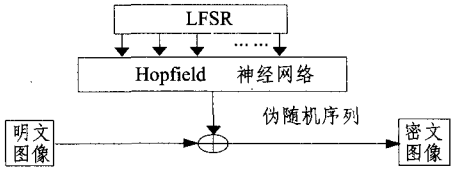

图 1 利用神经网络加密

元胞自动机具有时间、空间、状态的离散性和复杂的动力学性质，是与连续 Cantor 映射动力系统对应的离散动力系统，其组成单元简单，信息处理并行化，元胞单元的局部作用会引起复杂的全局变化。它的自组织性决定了所产生的序列具有一定的随机统计特性，利用它可以产生符合密码学要求的伪随机序列。文献[12]提出了一种基于二维可逆元胞自动机的多幅图像加密算法，该算法在加密过程中对多幅图像进行循环链式迭代，每幅图像按照密钥流序列选择不同的迭代规则和步数，明文图像和密文图像之间有复杂的依赖关系。

基于神经网络和元胞自动机的加密为图像加密的并行实现提供了方法。

2.6 基于盲源分离的加密

盲源分离是信号处理领域的热门课题，它在源信号和混合参数均未知的情况下，能够从混合信号中分离得到源信号的估计。当混合信号个数少于源信号个数时，通常不可能完全分开所有的源信号，这就是求解极为困难的盲源分离欠定难题，一些文献利用它来设计加密方法[13]，盲源分离图像加密的原理见图 2。

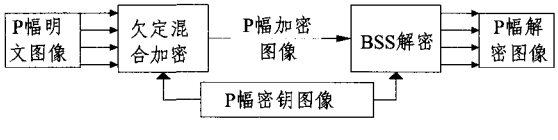

图 2 盲源分离图像加密原理[13]

由于盲源分离存在顺序和幅度模糊性，解密得到的图像可能发生顺序变化和像素值反转。并且，盲源分离通常无法分离强相关信号。当明文图像之间相关性较强时，在盲源分离解密之前，必须对加密图像信号进行去相关预处理，如高通滤波、多分辨率子带分解等，这增加了解密运算量。另外，基于盲源分离的图像加密要求密钥图像与明文图像大小相等、数目相同，这对密钥的设置与产生提出了更高的要求。所以，它不适合作为图像加密算法。

文献[14]利用盲源分离欠定难题提出一种多幅图像加密算法，它采用代数运算解决了不确定性和无法直接分离强相关图像的问题。像素的值域是有限整数集，而该算法并没有讨论如何处理密文图像中超出值域范围的像素，这可能导致解密存在很大的失真。另外，分析该算法的加解密运算可以发现它容易遭到选择明文攻击。

2.7 加密算法比较

上述 6 类加密算法以对应的主要操作(如置乱、生成混沌序列、空间域到变换域的转换等)为基本运算，综合比较的结果见表 1。

表 1 6 类加密算法定性比较

图像加密思路	安全性	计算复杂度	密文数据量
基于空间域的像素置乱	较低	小	等于明文
基于混沌的加密	高	较小	等于明文
基于变换域的加密	高	大	小于等于明文
基于秘密分割与秘密共享的加密	低	小	大于明文
基于神经网络和元胞自动机的加密	较高	中	等于明文
基于盲源分离的加密	中	较大	大于等于明文

3 现有图像加密算法的不足

3.1 没有综合运用置乱、代换、扩散

一些针对像素的空域加密算法看起来很复杂，但是没有综合运用置乱、代换、扩散操作，明密文对中存在很强的线性关系，它们容易受到选择明文攻击。

文献[15]提出的根据序列中元素的取值来控制图像进行自适应置乱的算法缺少代换和扩散操作。文献[16]对一种基于猫映射的加密算法进行了分析，指出了该算法在置乱过程中不改变像素值所导致的安全漏洞。文献[1]运用广义猫映射对图像进行加密，它含有置乱、代换、扩散操作并且迭代多轮，但由于该算法中的置乱操作存在不动点而且代换和扩散操作比较简单，导致明密文中存在一定程度的线性计算关系，因此它容易被破解。文献[17]提出了一种改变像素值的矩阵变换加密算法，它没有改变像素的位置，通过选择明文攻击求解同余方程组便可破解。文献[18]对现有的一个加密算法进行了分析，发现该算法的运算操作是线性的，而且整个算法等效于两个串行的操作步骤，通过一对明密文即可破解出等效密钥；该文根据 Logistic 映射构造了一种新的混沌系统用于加密，并且综合运用了位置置乱、扩散和代换操作，提高了安全性。

3.2 没有采用自适应加密的思想

一些加密算法对任何明文加密时，实际使用的都是相同的等效密钥，即没有充分利用明文的数据信息来影响等效密钥的产生，这样的算法容易被选择明文攻击。

文献[19]加密任意两幅明文图像 $p1$、$p2$ 时，相同位置的像素被置换到密图中相同的位置上，相同位置像素的代换操作数完全一样，而且像素之间没有扩散，这样只需任意两组

明、密文对即可分析出若干置乱映射对应位置和若干代换操作数。对 $N\times N$ 大小的灰度图进行选择明文攻击时，只需要选择 $\lceil(1+\sqrt{1+n^2/32})/2\rceil+1$ 个明文即可破解出所有的等效密钥。这一类算法不管把加密轮数提高到多少轮，安全性都不会提高。文献[5]也仅有“固定位置的置乱”与“固定操作数的代换”，没有扩散或者自适应的操作，安全性较低。文献[20]的加密算法可以分解为串行执行、互不影响的置乱和扩散操作，没有使用比较强的自适应加密，通过选择像素值全为0的图像就可以消除置乱的影响，进而可以破解出等效密钥。文献[21]对文献[22]的加密算法进行了分析，指出该算法没有与明文相关的自适应操作，通过选择明文攻击可以破解出等效密钥；它对该算法进行了改进，将图像数据通过一个不可逆的变换引入到加密过程中，大大提高了算法的安全性。

3.3 结合压缩的加密安全性有待提高

有的算法将加密过程与编码过程相融合，为了不影响压缩，采用的加密操作太简单，算法不安全。有的算法采用了选择加密的方法，即仅对变换域中少量的重要系数进行加密，攻击者可以通过忽略或者代换被加密的部分来窥探原始明文图像中的内容。

有的算法先以 8×8 大小的像素块为单位对图像进行像素块的置乱，然后将得到的图像进行离散余弦变换、量化，把此时所得到的量化后系数的符号位进行加密。由于该算法在置乱位置时以块为最小单位，而且在改变符号位时所用的操作太简单，因此它容易被选择明文攻击破解。

针对 JPEG 图像的加密，有的算法先对 Y、Cb、Cr 分量以 8×8 的 DCT 块为最小单位在分量内部分别进行置乱；然后在每个 8×8 的 DCT 块内按频率高低划分为 4 个区域，在各个小区域内进行 DCT 系数的置乱；最后根据混沌序列改变所有 DCT 系数的符号位。分析加密过程可以发现，通过比较明密文对中相同颜色分量的 DCT 系数分布就能发现置乱、改变符号位的规律，从而破解出等效密钥。

有的算法利用混沌序列与哈夫曼码表相异或，来达到加密 JPEG 图像的目的。该算法比较简单，通过一对明密文即可破解。

文献[23]将彩色图像的 R、G、B 分量按 8×8 大小分块，以块为单位分别进行空域置乱。该算法考虑到了加密操作对 JPEG 压缩编码的影响，使得加密尽量不影响压缩，但是算法仅有块与块的置乱，而且 RGB 3 种颜色数值之间没有置乱，导致安全性不高，容易受到已知明文攻击或选择明文攻击。

3.4 针对比特位的加密计算量太大

一些加密算法针对比特位单独进行操作，计算量较大。由于在内存中是以字节为单位存储数据的，计算机在处理每一个比特位时实际上需要耗费对整个字节进行操作的时间，因此总的计算量很大。

文献[24]先将二维图像($M\times N$)的像素值按比特位排列成二维矩阵，针对比特位进行置乱，然后将比特位拼凑成二维图像。该算法的安全性也不高，进行选择明文攻击时最多选择 8MN 个明文即可破解。文献[25]将像素的高 4 位比特平面分别置乱，将低 4 位比特平面统一置乱，然后对新图像中的像素值进行扩散。由于可以将该算法分解为互不影响、串行执行的置乱与扩散这两步，而且扩散操作的设计也给算法的破解留下了漏洞，因此通过选择明文攻击容易破解出所有的等效密钥。

4 数字图像加密展望

数字图像加密要求密文与明文的视觉效果完全不同，而且在保证加密算法具有很强的抗攻击能力的同时，实现快速的加密。后续可以从以下几方面进行研究，把它们适当地结合起来(见图 3)，设计出加密效果好、计算复杂度低、安全性高的算法。

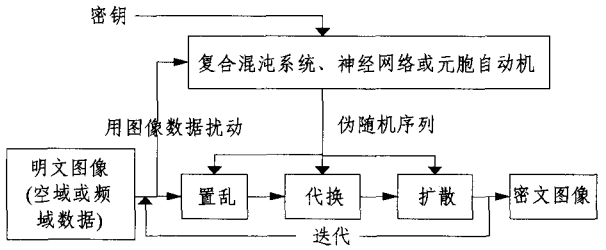

图 3 图像加密框架

①代换、扩散操作的设计。有些算法代换、扩散操作太简单，线形计算关系太强，导致加密算法容易被破解。需要研究适合图像加密的非线性的代换、扩散操作，这可以借鉴针对一维数据流的传统加密算法的设计思路，改造其中的具体加密部件以适用于操作像素，并且将置乱、代换、扩散 3 种操作有机地结合起来，使它们的优势互相补充。

②伪随机序列的生成。对于一些混沌密码算法，由于计算机精度有限，导致伪随机序列可能存在短周期，因此它们的安全性不够高。需要研究如何快速地产生具有更好随机性的伪随机数，这可以通过采用高维混沌系统、复合混沌系统等方法来实现。另外，也可以对神经网络和元胞自动机进行深入研究，利用它们来产生随机性好的序列。

③自适应加密。如果算法在加密过程中不仅依赖于密钥，而且一定程度上依赖于明文或者依赖于加密过程中产生的中间数据，那么选择明文攻击将更难成功，算法的安全性更高。需要研究计算量不大但是与明文密切相关的自适应加密算法。实际上，可以先利用传统加密算法加密由图像自适应产生的子密钥，然后再用所得结果进行真正加密图像的操作，这样就可以在略微增加计算量的情况下大大增强抵御选择明文攻击的能力。

④结合压缩编码的加密。目前已经有一些结合 JPEG、JPEG2000 压缩编码的数字图像加密算法，但其安全性不高；在存储、传输带宽受限的情况下，需要研究具有更高安全性而计算复杂度较小的压缩加密算法。

参 考 文 献

[1] 马在光，丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报，2003，24(2)：51-57

[2] 张瀚，王秀峰，李朝晖，等. 一种基于混沌系统及 Henon 映射的快速图像加密算法[J]. 计算机研究与发展，2005，42(12)：2137-2142

[3] Alvarez G，Li Shu-jun. Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption[J]. Communications in Nonlinear Science and Numerical Simulation，2009，14：3743-3749

[4] Chen T-H，Wu Chang-Sian. Compression-unimpaired batch-image encryption combining vector quantization and index compression[J]. Information Sciences，2010，180：1690-1701

(下转第 24 页)

[49] 颜佳,吴敏渊,陈淑珍. 跟踪窗口自适应的 Mean Shift 跟踪[J]. 光学精密工程,2009,17(10):2606-2010

[50] Ning Ji-feng, Zhang Lei, Zhang D, et al. Scale and Orientation Adaptive Mean Shift Tracking[J]. IET Computer Vision, 2012, 6(1):52-61

[51] Bradski G R. Real time face and object tracking as a component of a perceptual user interface[C]// IEEE Fourth Workshop on Applications of Computer Vision. 1998:214-219

[52] Li Xiao-he, Zhang Tai-yi, Shen Xiao-dong, et al. Object tracking using an adaptive Kalman filter combined with mean shift[J]. SPIE Journal of Optical Engineering, 2010, 49(2)

[53] 王江涛,杨静宇. 遮挡情况下基于 Kalman 均值偏移的目标跟踪[J]. 系统仿真学报,2007,19(18):4216-4220

[54] Wang Fang-lin, Yu Sheng-yang, Yang Jie. Robust and efficient fragments-based tracking using mean shift[J]. AEU-International Journal of Electronics and Communications, 2010, 64(7): 614-623

[55] Fang Jiang-xiong, Yang Jie, Liu Hua-xiang. Efficient and robust fragments-based multiple kernels tracking[J]. AEU-International Journal of Electronics and Communications, 2011, 65(11):915-923

[56] 颜佳,吴敏渊,陈淑珍,等. 应用 Mean Shift 和分块的抗遮挡跟踪[J]. 光学精密工程,2010,18(6):1413-1418

[57] Maggio E, Cavallaro A. Accurate appearance-based Bayesian tracking for maneuvering targets[J]. Computer Vision and Image Understanding, 2009, 113(4):544-555

[58] Li Shu-xiao, Chang Hong-xing, Zhu Cheng-fei. Adaptive pyramid mean shift for global real-time visual tracking[J]. Image and Vision Computing, 2010, 28(3):424-437

[59] Liangfu L, Zuren F, Weidong C, et al. A coarse-to-fine kernel matching approach for mean-shift based visual tracking[J]. Opto-Electronics Review, 2009, 17(1):65-71

[60] Shen Chun-hua, Brooks M J, van den Hengel A. Fast Global Kernel Density Mode Seeking: Applications to Localization and Tracking[J]. IEEE Transactions on Image Processing, 2007, 16(5):1457-1469

[61] 朱胜利,朱善安,李旭超,等. 快速运动目标的 Mean shift 跟踪算法[J]. 光电工程,2006,33(5):66-70

[62] 李弟平,邹北骥,傅自刚. 结合粒子滤波与 Mean Shift 的高速运动目标跟踪[J]. 小型微型计算机系统,2011,32(8):1665-1668

[63] Nummiaro K, Koller-Meier E, Gool L V. An adaptive color-based particle filter[J]. Image and Vision Computing, 2003, 21(1):99-110

[64] Yao An-bang, Wang Gui-jin, Lin Xing-gang, et al. An incremental Bhattacharyya dissimilarity measure for particle filtering[J]. Pattern Recognition, 2010, 43(4):1244-1256

(上接第 9 页)

[5] Gao Tie-gang, Chen Zeng-qiang. A new image encryption algorithm based on hyper-chaos[J]. Physics letters A, 2008(372): 394-400

[6] Tao Ran, Meng Xiang-yi, Wang Yue. Image encryption with multiorders of fractional Fourier transforms [J]. IEEE Transaction on Information Forensics and Security, 2010, 5(4):734-738

[7] Li Xin-xin, Zhao Dao-mu. Optical color image encryption with refined fractional Hartley transform[J]. Optik, 2010, 121(7): 673-677

[8] Zhou Nan-run, Wang Yi-xian, Gong Li-hua. Novel optical image encryption scheme based on fractional Mellin transform [J]. Optics Communications, 2011, 284(13):3234-3242

[9] Zhou Nan-run, Dong Tai-ji, Wu Jian-hua. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform [J]. Optics Communications, 2010 (283): 3037-3042

[10] Sudharsanan S. Shared Key Encryption of JPEG Color Images [J]. IEEE Transactions on Consumer Electronics, 2005, 4(51): 1204-1211

[11] 丁群,陆哲明,孙晓军. 基于神经网络密码的图像加密[J]. 电子学报,2004,32(4):677-679

[12] 平萍. 元胞自动机原理及其在密码学的应用研究[D]. 南京:南京理工大学,2009

[13] Lin Qiu-hua, Yin Fu-liang, Mei Tie-min, et al. A Blind Source Separation-based Method for Multiple Image Encryption[J]. Image and Vision Computing, 2008, 26:788-798

[14] 林秋华,党杰,殷福亮. 盲源分离图像加密的相关运算解密法[J]. 通信学报,2008,29(1):109-114

[15] Chen Gang, Zhao Xiao-yu, Li Jun-li. A Self-Adaptive Algorithm on Image Encryption[J]. Journal of Software, 2005, 16(11): 1975-1982

[16] Xu Shu-jiang, Wang Ying-long, Wang Ji-zhi, et al. Cryptanalysis of Two Chaotic Image Encryption Schemes Based on Permutation and XOR Operations [C] // Proceedings of International Conference on Computational Intelligence and Security 2008. Washington D C: IEEE Press, 2008:433-437

[17] Acharya B, Patra S K, Panda G. Image Encryption by Novel Cryptosystem Using Matrix Transformation[C]//First International Conference on Emerging Trends in Engineering and Technology, 2008. Washington D C: IEEE Press, 2008:77-81

[18] Sam I S, Devaraj P, Bhuvaneswaran R S. A novel image cipher based on mixed transformed logistic maps[J]. Multimedia Tools and Appl, 2012, 56(2):315-330

[19] Guan Zhi-hong, Huang Fang-jun, Guan Wen-jie. Chaos-based image encryption algorithm[J]. Physics Letters A, 2005, 346(1-3):153-157

[20] Zhang Guo-ji, Liu Qing. A novel image encryption method based on total shuffling scheme[J]. Optics Communications, 2011

[21] Deng Shao-jiang, Zhan Yan-ping, Xiao Di, et al. Analysis and improvement of a hash-based image encryption algorithm[J]. Communications in Nonlinear Science and Numerical Simulation, 2011(16):3269-3278

[22] Cheddad A, condell J, Curran K, et al. A Hash-based image encryption algorithm[J]. Opt Commun, 2010(283):879-893

[23] 王英,郑德玲,王振龙. 空域彩色图像混沌加密算法[J]. 计算机辅助设计与图形学学报,2006,18(6):876-880

[24] Ye Guo-dong. Image scrambling encryption algorithm of pixel bit based on chaos map[J]. Pattern Recognition Letters, 2010 (31):347-354

[25] Zhu Zhi-liang, Zhang Wei, Wong K-w, et al. A chaos-based symmetric image encryption scheme using a bit-level permutation [J]. Information Sciences, 2011(181):1171-1186