(a) H_1 增加 0.1 后的密文图像　　(b) H_2 增加 0.1 后的密文图像

(c) H_1 变化前后的密文差别图　　(d) H_2 变化前后的的密文差别图

图 6. 384*256 图像的密钥微小变化前后的密文图像和密文差别图像

Fig.6　The ciphertext images after the keys changing and the ciphertext difference images before and after key changing (the size of the images are 384*256 pixels) ((a) The ciphertext image after the key H_1 increasing 0.1；　(b) The ciphertext image after the key H_2 increasing 0.1；　(c) The ciphertext difference image before and after the key H_1 changing; (d) The ciphertext difference image before and after the key H_2 changing)

表五　密钥微小变化前后的密文图像之间的相关性和相似度

Table 5　The correlation and SSIM of the ciphertext images before and after the keys changing

	K_0-K_1	K_0-K_2
相关性	0.0045	0.0091
相似度(SSIM)	0.0008	0.0007

4.2.7 差分分析

在相同的密钥条件下，差分分析研究明文的定量改变对密文的影响程度。分别用 $P_0, P_0+\Delta P, C_{P_0}, C_{P_0+\Delta P}$ 表示明文和改变了的明文图像以及对应的密文图像，差分分析的一般方法是对于微小的改变 ΔP，比较相同密钥条件下 C_{P_0} 和 $C_{P_0+\Delta P}$ 之间的差异。若 C_{P_0} 和 $C_{P_0+\Delta P}$ 具有较大差异则说明加密算法抵御差分攻击的能力是强大的。

将 Tiger, Beauty, House 三幅图像的灰度值分别增加 0.1，计算灰度改变前后同一组密钥对应的两幅密文图像的相关系数和相似度的绝对值，参见表六；从中发现密文图像的相关性和结构相似度均接近于 0，这表明算法能有效地抵御差分攻击。

表六　明文微小变化前后对应的密文图像之间的相关性和相似度

Table 6　The correlation and SSIM of the ciphertext images before and after the plaintext changing

	Tiger	Beauty	House
相关性	0.0019	0.0011	0.0029
相似度(SSIM)	0.000070	0.000009	0.000027

5 结　论

本文的图像混合加密方案综合运用了 H-S 混沌映射、矩阵点运算、矩阵非线性复合变换等知识。通过混沌密钥矩阵、序列随机排序和矩阵点运算构造的 λ 变换实现像素的置乱加密，将置乱加密的结果再次进行不同参数的 λ 变换和 β 变换实现灰度加密。由于混沌密钥矩阵和非线性运算的作用，混合加密算法具有一次一密的特点，足以保障算法有足够大的密钥空间抵御各类攻击；算法复杂度低、流程简单便于程序实现；算法可应用于任意大小的矩形图像加密，具有广泛的适应性；算法针对不可逆混沌映射设计，规避了传统混沌加密算法对映射的可逆性要求，有效地拓展了不可逆混沌映射的应用范围；加密仿真实验说明了混合加密技术的可行性和有效性，加密性能分析则表明了算法的安全性和鲁棒性，与混沌置乱加密、改进的标准映射置乱加密的结果比对分析则体现了本文算法的优越性。

大小 384*256 的图像 Tiger 的主要实验数据如下：密钥空间大小约为 212bit，远大于安全值 128bit；密文信息熵达到 7.9588 接近理想值 8.0000；密文与明文图像的相关系数仅为 0.0011，几乎不相关；两个主要密钥 H_1, H_2 变化前后得到的密文的相关系数分别为 0.0045 和 0.0091，结构相似指数分别为 0.0008,0.0007，算法对密钥变化非常敏感；明文像素变化前后得到的密文相关系数为 0.0019，结构相似度指数为 0.000070，算法能够有效防御差分攻击。

必须说明的是，密钥参数对加密性能的影响作用需要大量的仿真实验作为基础才能开展全面分析，此问题另行讨论。

参考文献 (References)

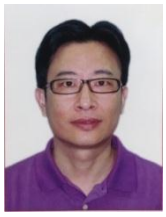
[1] Guan Z H, Huang F J, Guan W J. A chaos-based image encryption algorithm[J]. Physics Letters A, 2005, 346(1-3): 153-157.

[2] Tong X J, Cui M G. Image encryption with compound chaotic sequence cipher shifting dynamically[J]. Image and Vision Computing, 2008, 26(6): 843-850.

[3] Wei X P, Guo L, Zhang Q, et al. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system[J]. The Journal of Systems and Software, 2012, 85(2): 290-299.

[4] Kanso A, Ghebleh M. A novel image encryption

algorithm based on a 3D chaotic map[J]. Communications in Nonlinear Science Numerical Simulation, 2012, 17: 2943-2959.
[5] Zhu Z L, Zhang W, Wong K W, et al. A chaos-based symmetric image encryption scheme using a bit-level permutation[J] Information Science, 2011, 181: 1171-1186.
[6] Sasidharan S, Philip D S. A fast partial image encryption scheme with wavelet transform and RC4[J]. International Journal of Advances in Engineering &Technology, 2011,1(4):322-331.
[7] Schneier B. Applied Cryptography: Protocols, Algorithm and Source Code in C[M]. 2nd ed. New York: John Wiley &Sons, Inc, 1995: 38-144.
[8] Ahmad M, Farooq O. Chaotic image encryption algorithm based on frequency domain scrambling[J]. Information Processing Letters, 2010, 3(6): 76-82.
[9] Xiehua S. Image Encryption Algorithms and Practices with Implentations in C#[M]. Beijing: Science Press, 2013：21-148. [孙燮华. 图像加密算法与实践——基于 C#语言实现[M]. 北京：科学出版社，2013：21-148]
[10] Han S H, Yang S Y. An asymmetric image encryption based on matrix transformation[J]. ECTI Transactions on Computer and Information Technology, 2005, 1(2):126-133.
[11] Prasad M, Sudha K L. Chaos image encrypton using pixel shuffling[M]. 2nd ed. Wyld C: CCSEA, CS &IT, 2011:169-179.
[12] Chen Yucheng, Ye Ruisong. A novel image Encryption algorithm based on improved standard mapping[J]. Computer Science and Application, 2017, 7(8):753-773. [陈裕城，叶瑞松. 基于改进标准映射的图像加密算法[J]. 计算机科学与应用，2017, 7(8):753-773.]
[13] Huang C K, Nien H H. Multi chaotic systems based pixel shuffle for image encryption[J]. Optics Communications, 2009,282: 2123-2127.
[14] Contour Detection and Image Segmentation Resources[DB/OL]. 2018-09-09[2018-08-10]. https://www2.eecs.berkeley.edu/Research/Projects/CS/vision/grouping/resources.html.
[15] Patidar, V., Pareek, N.K., Purohit, G., et al. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption[J]. Optics Communications, 2011, 284: 4331-4339.



梁锡坤，1968 年生，男，博士，副教授，主要研究方向为图像加密，数字图像处理，智能信息处理等。
E-mail: schenken@163.com.

陶利民，1975 年生，男，博士，讲师，主要研究方向为应用密码学，服务计算，云计算。
E-mail: tlm5460@163.com.

胡　斌，1978 年生，男，博士，副教授，主要研究方向为应用密码学，网络与信息安全。
E-mail: tinrant@163.com.