基于像素对匹配的大容量SAR数据信息隐藏算法

刘娟妮， 周 诠
(西安空间无线电技术研究所空间微波技术国家级重点实验室，西安，710100)

摘要 针对SAR数据提出一种参考秘密信息内容对载体像素对匹配的大容量信息隐藏方法。该方法利用提取函数将SAR数据实部和虚部的不同组合结果映射为一位n^2进制信息，并通过不同组合结果的优选使含密SAR数据与原载体数据的MSE最小，保证SAR原始数据成像质量几乎不受影响。实验对比结果证明：与同类隐藏方法相比，在信息嵌入量相同时，该隐藏算法PSNR平均提高0.7 dB，且像素对组合模式可以作为密钥用于接收端信息提取，利用载体的不同组合方法可以有效提高算法的安全性。

关键词 信息隐藏；合成孔径雷达；像素对匹配；隐藏容量
DOI 10.3969/j.issn.1009-3516.2015.04.017
中图分类号 TN957.52 **文献标志码** A **文章编号** 1009-3516(2015)04-0070-04

An Algorithm of High Capacity Information Hiding Based on Pixel Pair Matching for SAR Raw Data

LIU Juanni, ZHOU Quan
(National Key Laboratory of Science and Technology on Space Microwave, Xi′an Institute of Space Radio Technology, Xi′an 710100, China)

Abstract: Aimed at SAR raw data, this paper proposes a high capacity information hiding algorithm based on pixel pair matching conducted according to the secret data. By using an extraction function, different combination of SAR real part and imaginary part are mapped into a secret digit in an n_2-ary notation system, and the optimal combination is chosen for a data block with the smallest MSE. Thus, the distortion caused by information hiding can be ignored for SAR imaging. Compared with the other similar algorithms, the PSNR of the proposed method increases 0.7 dB on average under condition of the same capacity, and high security is achieved with the help of various combinations.

Key words: information embedding; synthetic aperture radar; pixel pair matching; hiding capacity

信息隐藏作为卫星隐蔽通信的新手段[1]，可以将一些重要数据隐藏在SAR遥感数据中通过公开的卫星信道传输，在不增加传输速率的前提下达到隐蔽通信的目的，为卫星通信提供一种安全的信息传输途径。

空域隐写方法最具代表性的算法是最低有效位替代法[2]，和基于LSB的优化像素调整方法OPAP，都是利用一个载体像素来隐藏r位秘密信息。另一类空域隐写方法是利用一个像素对来完成信息隐藏，例如LSB匹配重访算法LSBMR[4]提出基于方向调整的EMD算法[5]。LSBMR最多只需要修改像素对中一个像素值就可以隐藏2 bit秘密信息，因而图像质量进一步提高。EMD算法是对LSBMR的改进，通过增加像素修改方向使得一个

收稿日期：2015-03-23
基金项目：国家自然科学基金资助项目(61372175)；国家重点实验室基金资助项目(9140C530403130C53192)
作者简介：刘娟妮(1985—)，女，陕西西安人，博士生，主要从事信息隐藏及图像处理研究.E-mail：liujuanni@126.com

引用格式：*刘娟妮，周诠. 基于像素对匹配的大容量SAR数据信息隐藏算法[J]. 空军工程大学学报：自然科学版，2015，16(4)：70-73. LIU Juanni，ZHOU Quan. An Algorithm of High Capacity Information Hiding Based on Pixel Pair Matching for SAR Raw Data[J]. Journal of Air Force Engineering University：Natural Science Edition，2015，16(4)：70-73.*

像素对可以隐藏一位 5 进制的秘密信息，隐藏容量从 1 bpp 提高到 $(1/2)\log_2 5=1.161$ bpp，然而这 2 个算法的最大嵌入容量无法再增加，因此不适合大容量信息隐藏应用。最近，很多研究者提出不同的 EMD 改进算法[6-8]，有些通过组合不同编码方法来提高隐藏容量，有些利用优化方法来改善含密图像质量。2011 年，Kieu 等[7] 提出的 Fully EMD (FEMD)算法借助 EMD 思想，通过增加像素可修改区域来提高隐藏容量。该算法的隐藏容量为 $C=\log_2 n$ 。

为了进一步改善含密图像质量，本文提出以 SAR 数据为载体的大容量信息隐藏算法。

1　本文算法

1.1　像素对匹配优化

由于 FEMD 算法安全性差，一旦隐藏方法被识破，秘密信息将被完全提取。为了增强算法的安全性，本文利用 2 种方法来改善。首先在预处理阶段，利用置乱算法（如 Arnold 置乱[9]）或混沌序列对载体 SAR 数据进行加密，掩盖信息隐藏的位置；其次在信息隐藏过程中，利用像素对匹配优化方法将秘密信息隐藏在 8 种不同组合方式得到的像素对中，组合方式结果作为密钥用于接收端信息提取。

像素对匹配优化方法为：将 SAR 数据分为 8×8 大小的数据块，每个数据块按图 1 的 4 种方式进行实部 R 和虚部 I 的交叉组合及各自组合（阴影图案相同的 2 个数据组成 1 个像素对）。每种情况像素对数据交换将构成另外 4 种组合结果。采用这 8 种不同的组合方式分别进行信息隐藏，选择公式(7)定义的 MSE 最小的情况作为最终隐藏结果，可以认为此时像素对与秘密信息的匹配度最高。

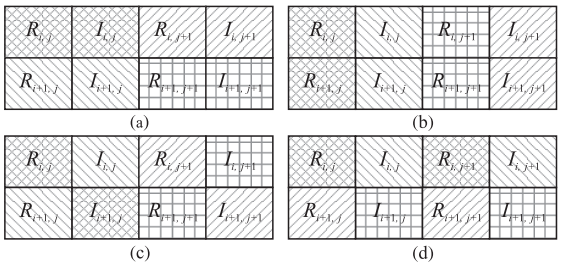


图 1　数组组合示意图

Fig.1　Examples for data combination

在接收端，为了正确提取秘密信息，需要每个数据块中组合方式的标识信息，可以用 3 bit 来表示 8 种组合方式：‘000’～‘011’分别表示图 1(a)～(d) 4 种情况，‘100’～‘111’表示像素对数据交换的 4 种情况。只有授权的接收者在得到正确的数据组合信息后才能正确获取秘密信息，这些标识数据可以作为密钥单独传输或者直接隐藏在载体数据中传输。对于大容量信息隐藏（$n=16$），这些标识数据可以忽略不计。假设载体数据大小为 512×512，图像分块个数为 64×64，总的标识数据量为 12 288 比特，仅占总隐藏比特数 1 048 576 的 1%。

1.2　嵌入过程

本文信息隐藏步骤如下：

Step1　将二进制信息转为 n^2 进制。每 L 位二进制数转换为 K 位 n^2 进制，两者取值关系为：

$$L=\lfloor K\log_2 n \rfloor \tag{1}$$

当 $n=2^k$ 时，可以用 1 位 n^2 进制信息完全表示 k 位二进制信息，即 $K=1$，$L=k$。

Step2　SAR 数据预处理。利用 Arnold 算法将 SAR 数据置乱，或者用混沌序列对数据进行调制。

Step3　预处理后的数据分成 8×8 大小数据块并按照 1.1 节方法组合实部和虚部。

Step4　对每个分块数据的每一种组合方式分别执行如下步骤：

$$f(x,y)=[(n-1)x+ny]\bmod n^2 \tag{2}$$

1）取出一个像素对(x, y)，计算式(2) 的函数值 f 并和 1 位秘密信息 s 比较：如果 $f=s$，则不改变像素对(x, y)，否则按下面规则修改像素对：遍历式(3)～(4)定义的集合 X 和 Y，搜索满足 $f(x+\Delta x,y+\Delta y)=s$ 的像素对 $(x+\Delta x,y+\Delta y)$，选择其中修改量 $(\Delta x,\Delta y)$ 最小的作为结果：

$$X=\{\Delta x\in Z\,|-q\leqslant\Delta x\leqslant q\} \tag{3}$$

$$Y=\{\Delta y\in Z\,|-q\leqslant\Delta y\leqslant q\} \tag{4}$$

2）若含密像素对(x', y')溢出，则按式(5)调整，然后重新嵌入秘密信息：

$$\begin{cases}x=x+1, & x'<0\\ y=y+1, & y'<0\\ x=x-1, & x'>255\\ y=y-1, & y'>255\end{cases} \tag{5}$$

3）按 Z 字扫描顺序重复执行 1）和 2），完成该数据块其他像素对的隐藏。

Step5　按式(7)分别计算 8 种组合方式的 MSE，选择最小值对应的隐藏结果为该分块的最终结果，并将标识信息记录在表中。

Step6　重复 **Step4～6**，直至嵌入所有信息。

Step7　对含秘数据进行反置乱或用混沌序列恢复数据顺序。

1.3　提取过程

秘密信息的提取方法步骤为：①采用与隐藏过程相同的预处理方法处理含密数据；②将数据按 8

×8 大小分块,并从表中提取该块数据组合方式的指示符;③根据指示符重新组合该块数据,并按照公式(2)提取 32 位 n^2 进制秘密信息;④将提取的 n^2 进制信息转为二进制信息;重复执行步骤③和④,直至信息提取完毕。

2 实验结果

实验使用 MATLAB2011a 平台,主频 2.50 GHz,内存大小为 2 GB。载体数据包括 RadarSat-1[10] SAR 数据和 6 幅 512×512 的标准灰度图像(如图 2 所示)。SAR 数据是实部虚部间隔存储的,选取 4 幅 1 536×2 048 大小的数据块并量化为 8 bit 进行实验。n^2 进制秘密信息用伪随机数发生器产生,隐藏前载体数据进行 Arnlod 置乱,置乱次数 $N=50$。如果需要更高的安全性,可以采用混沌序列或一些加密算法对载体进行预处理。

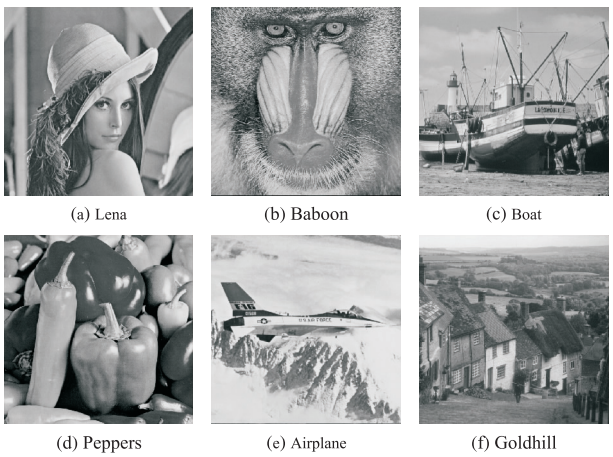
使用峰值信噪比 PSNR 和隐藏容量 C 来衡量隐藏算法的性能。对于一幅大小为 $H\times W$ 的 8 bit 数字图像,PSNR 为:

$$\mathrm{PSNR}=10\lg\frac{255^2}{\mathrm{MSE}}\mathrm{dB} \tag{6}$$

式中:MSE 为原图像与含密图像之间的均方差,计算公式为:

$$\mathrm{MSE}=\frac{1}{HW}\sum_{i=1}^{H}\sum_{j-1}^{W}(x_{ij}-\bar{x}_{ij})^2 \tag{7}$$

式中:x_{ij},$\bar{x}_{ij}$ 分别表示原始图像和含秘图像在(i,j)处的像素值。



(a) Lena (b) Baboon (c) Boat

(d) Peppers (e) Airplane (f) Goldhill

图 2 测试图像

Fig.2 Test images

2.1 SAR 数据实验结果

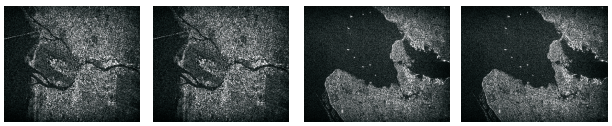
参数 n 影响信息隐藏容量。表 1 给出了 $n=2^k$ 时,4 组 SAR 数据的 PSNR 对比结果。从表中数据可以看出,4 组不同 SAR 数据的 PSNR 取值与载体数据差异关系不大,主要和嵌入容量相关,PSNR 随着 C 的增加而降低,隐藏容量 C 每增加 1 bpp,PSNR 降低约 6 dB。

表 1 SAR 数据的隐藏容量 C 和 PSNR

Tab.1 Hiding capacity C and PSNR for SAR data

n	2	4	8	16
C	1	2	3	4
Data1	53.072	47.471	41.599	35.447
Data2	53.068	47.472	41.601	35.455
Data3	53.072	47.472	41.621	35.461
Data4	53.075	47.464	41.598	35.432
均值	53.072	47.470	41.605	35.449

为了研究本文隐藏算法是否对成像结果造成影响,用经典 RD 成像算法对含密 SAR 数据进行成像,并和未隐藏数据的成像结果进行对比。图 3 列举了 Data1 及 Data2 原始数据与含密数据成像对比结果,每组数据隐藏前后成像结果的 MSE 及 PSNR 见表 2。总体来说,在信息嵌入率高达 1/2 时,含密数据的成像结果与原始数据成像结果的 PSNR 均高于 30 dB,仍然满足视觉要求。



(a) Data1 (b) 含密Data1 (c) Data2 (d) 含密Data2

图 3 成像对比结果($n=2$)

Fig.3 Comparison results of RD imaging ($n=2$)

表 2 隐藏前后数据成像结果的 MSE/PSNR

Tab.2 The MSE/PSNR of imaging results using original and stego SAR data

n	2	4	8	16
C	1	2	3	4
Data1	1.39/46.701	4.48/41.623	16.51/35.954	64.51/30.035
Data2	0.97/48.267	3.34/42.892	10.87/37.77	44.11/31.686
Data3	0.40/52.107	1.11/47.660	3.29/42.953	12.65/37.111
Data4	0.43/51.845	1.08/47.783	3.74/42.401	13.23/36.915

2.2 标准图像实验结果

表 3 是 6 幅测试图像在不同 n 值时的隐藏容量 C 和图像质量结果。可以看出,本文算法在嵌入 4 bpp 秘密信息时,PSNR 仍然高达 35.5 dB,表明本文算法获得的含密图像质量较好;不同类型图像的实验结果很近似,说明本文算法对载体的适应性很好,而且信息隐藏容量仅与图像大小及参数 n 有关,这使算法具有很强的实用性。

另外，以 Lena 图像为例将本文算法和其他同类算法进行对比，结果见图 4。可以看出，本文算法和 FEMD 算法可以实现更多不同嵌入率的信息隐藏，而且本文算法的 PSNR 均优于其他算法。与 LSBs 算法相比，PSNR 平均增加 3.1 dB，与 FEMD 相比 PSNR 增加了 0.7 dB。图像质量改善的原因在于：本文算法采用了像素对匹配优化方法，将载体数据按不同方式组合，增加了载体像素对和秘密信息匹配的几率。

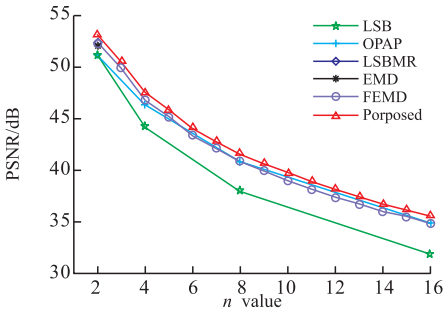


图 4　算法对比结果

Fig.4　Comparison results of different algorithms

表 3　不同 n 值的隐藏容量 C 和 PSNR

Tab.3　Hiding capacity C and PSNR of proposed method with different n

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
C	1	1.59	2	2.23	2.59	2.81	3	3.17	3.32	3.46	3.59	3.7	3.81	3.91	4
Lena	53.075	50.470	47.471	45.792	44.101	42.786	41.600	40.656	39.664	38.880	38.080	37.414	36.638	35.984	35.446
Baboon	53.075	50.468	47.472	45.790	44.107	42.795	41.627	40.685	39.701	38.923	38.128	37.472	36.653	36.003	35.515
Boat	53.074	50.466	47.475	45.790	44.093	42.788	41.603	40.654	39.654	38.863	38.047	37.386	36.671	36.014	35.474
Airplane	53.075	50.462	47.453	45.781	44.062	42.773	41.591	40.619	39.623	38.824	38.012	37.347	36.706	36.034	35.480
Goldhill	53.072	50.465	47.476	45.789	44.099	42.794	41.623	40.664	39.691	38.897	38.097	37.436	36.615	36.013	35.494
Peppers	53.069	50.462	47.471	45.787	44.099	42.792	41.611	40.682	39.702	38.918	38.112	37.447	36.639	35.993	35.475
均值	53.073	50.466	47.467	45.788	44.093	42.788	41.610	40.660	39.673	38.884	38.079	37.417	36.654	36.007	35.481

2.3　计算量分析

本文通过像素对 8 种组合方式的优化来获得含密图像 PSNR 的改善，因此算法计算量相应有所增加。与同类算法运行时间的对比结果见表 4。实验所用载体图像大小为 512×512，每种算法的嵌入率均为 1 bpp。相比其他算法，本文算法的运行时间最长，耗时最多的主要是嵌入过程，这是因为对每个数据块都需要按不同组合方式进行 8 次 FEDM 隐藏。可以根据不同应用场合择优选择隐藏方法，对实时性要求较高时可以采用文献[5～6]的方法，如果需要秘密信息具有高安全性的同时获得更高的成像质量则可以采用本文方法。

表 4　$n=2$ 时算法运行时间对比　（单位：秒）

Tab.4　Comparison of execution time with $n=2$　(s)

算法	平均嵌入时间	平均提取时间	总运行时间
EMD[5]	1.61	0.48	2.10
FEDM[6]	7.54	0.47	8.07
本文算法	92.23	1.35	93.83

3　结语

本文针对 SAR 原始数据提出一种大容量空域信息隐藏方法，给出了 SAR 数据隐藏容量与成像质量的实验结果，通过载体像素对匹配优化提高隐藏性能及算法的安全性，可以实现各种不同容量信息的隐藏。当 $n=2^k$ 时，每个像素可以隐藏 k bit 秘密信息，等价于 LSBs 方法，但是图像的 PSNR 平均提高 3 dB。和其他同类方法相比，本文方法在隐藏容量和 PSNR 两方面的性能均得到提高。

参考文献(References)：

[1] 李晓博，周诠. 基于直方图修改的卫星遥感图像无损隐藏传输[J]. 宇航学报，2013，34(5)：686-692.
LI Xiaobo，ZHOU Quan. A Iossless Data Hiding Transmission Method for Satellite Remote Sensing Image Based on Histogram Modification [J]. Journal of Astronautics，2013，34(5)：686-692.(in Chinese)

[2] Bender W，Gruhl D，Morimoto N，et al. Techniques for Data Hiding [J]. IBM System Journal，1996，35(3-4)：313-336.

[3] Chan C K，Cheng L M. Hiding Data in Images by Simple LSB Substitution [J]. Pattern Recognition，2004，37(3)：469-474.

[4] Mielikainen J. LSB Matching Revisited [J]. IEEE Signal Processing Letters，2006，13(5)：285-287.

[5] Zhang X P，Wang S Z. Efficient Steganographic Embedding by Exploiting Modification Direction [J]. IEEE Communications Letters，2006，10(113)：781 - 783.

[6] Kieu T D，Chang C C. A Steganographic Scheme by Fully Exploiting Modification Directions [J]. Expert Systems with Applications，2011，38(8)：10648-10657.

[7] Qin C，Chang C C，Hsu T J. Reversible Data Hiding Scheme Based on Exploiting Modification Direction with Two Steganographic Images [J]. Multimedia Tools and Applications，2014：1-12.

[8] Shen S Y，Huang L H. A Data Hiding Scheme Using Pixel Value Differencing and Improving Exploiting Modification Directions [J]. Computers & Security，2015，48：131-141.

[9] 吴成茂. 离散 Arnold 变换改进及其在图像置乱加密中的应用 [J].物理学报，2014，63(9)：090504.
WU Chengmao. An Improved Discretearnold Transform and Its Application in Image Scrambling and Encryption [J]. Acta Physica Sinica，2014，63(9)：090504.(in Chinese)

[10] Cumming I G，Wong F H. Digital Processing of Synthetic Aperture Radar Data：Algorithms and Implementation [M]. Norwood：Artech House，2005.

（编辑：徐敏）