

# 军事图像加密通信中数据隐藏算法研究与仿真

岳鑫, 周城, 甘文道, 张铭隆

(重庆通信学院, 重庆 400035)

**摘要:** 在对军事通信图像加密通信中的数据进行隐藏的过程中, 数据融入方式是通过依据某种规律曲线的顺序扫描待隐藏数据的单元来实现的, 导致传统的融合军事图像加密通信中数据隐藏算法, 由于检测工具有规律可循, 不容易逃脱检测, 无法对军事图像数据进行有效的隐藏。提出一种采用随机融入方式的 reversible 数据隐藏算法, 直接提取军事图像边缘特征, 充分挖掘军事图像视觉屏蔽特性, 通过军事图像分块方差对其边缘特性进行刻画, 确保军事图像边缘的完整度, 构建军事图像采样子图与参照子图间的军事差图, 通过数据隐藏的提取方法, 将隐藏军事图像差图数据合成相应的数据隐藏码流, 完成所有军事差图的置乱操作, 将置乱后的军事差图中的隐藏数据按照数据隐藏的正确率进行度量, 实现军事图像加密通信中的数据隐藏。仿真结果表明, 采用所提方法对军事图像加密通信中的数据进行隐藏的效果与隐藏容量均优于传统方法, 验证了所提方法的有效性。

**关键词:** 军事图像; 加密通信; 数据隐藏

**中图分类号:** TP391.9      **文献标识码:** B

## Research and Simulation of Data Hiding Algorithm in Military Image Encryption Communication

YUE Xin, ZHOU Cheng, Gan Wen - dao, ZHANG Ming - long

(Chongqing Communication Institute, Chongqing 400035, China)

**ABSTRACT:** The paper presented a reversible data hiding algorithm using random integrated mode. Edge features of military image were directly extracted to fully excavate the visual masking properties of military image. Through military image block variance, the edge features was depicted, ensuring the integrity of the military image edge. The acquired sub-image of military image and the military difference image between reference sub-images were constructed. Through the extraction method of data hiding, the hiding data of difference image in military image were composed to form the corresponding data hidden code stream, to complete the scrambling operations of all military difference images. The hiding data in military figure after scrambling were measured according to the accuracy of the data hiding, to realize the data hiding of military image encryption communication. The simulation results show that the effect and hiding capacity of using proposed method for the data hiding in military image encryption communication are superior to traditional methods, verifying the effectiveness of the proposed method.

**KEYWORDS:** Military image; Encryption communication; Data hiding

### 1 引言

信息隐藏技术是指将特定信息隐藏在数字化宿主信息中的方法。随着信息处理技术与通信手段的不断发展, 关系国家安全、军事通信等方面的信息安全更加突出, 使得信息隐藏技术成为信息技术研究的热点之一, 广泛应用于军事领

域中<sup>[1-2]</sup>。在对军事图像加密通信中的数据进行隐藏的过程中, 数据融入方式是通过依据某种规律曲线的顺序扫描待隐藏数据的单元来实现的, 导致传统的基于融合的军事图像加密通信中数据隐藏算法由于检测工具有规律可循, 不容易逃脱检测<sup>[3-5]</sup>, 无法对军事图像数据进行有效的隐藏。本文提出一种采用随机融入方式的 reversible 数据隐藏算法, 直接提取军事图像边缘特征, 充分挖掘军事图像视觉屏蔽特性, 通过军事图像分块方差对其边缘特性进行刻画, 确保军事图像边缘的完整度, 构建军事图像采样子图与参照子图间的军事差图, 通过数据隐藏的提取方法, 将隐藏军事图像差图数据合成相应的数据隐藏码流, 完成所有军事差图的置乱操作, 将

基金项目: 基于广义骑士巡游的图像和视频加密与压缩同步算法研究 (61272043); 基于图论和数论的图像和视频加密与压缩同步技术研究 (cstc2013jjB40009)

收稿日期: 2014-06-26

置乱后的军事差图中的隐藏数据按照数据隐藏的正确率进行度量,实现军事图像加密通信中的数据隐藏。仿真结果表明,采用所提方法对军事图像加密通信中的数据进行隐藏的效果与隐藏容量均优于传统方法,验证了所提方法的有效性。

## 2 融合的军事图像加密通信

### 2.1 基于融合的图像数据隐藏技术

在对计算机图形进行设计的过程中通常采用调配函数方法<sup>[6]</sup>。假设空间中一共有  $n+1$  个点  $P_0, P_1, \dots, P_n$ , 则将  $\{P_i | i = 0, 1, \dots, n\}$  作为控制点的  $n$  次 B-spline 曲线可用式 (1) 描述

$$P(t) = \sum_{i=0}^n P_i B_i^n(t) \quad (1)$$

式中  $B_i^n(t)$  表示 B-spline 基函数

$$B_i^n(t) = \begin{bmatrix} n \\ i \end{bmatrix} (1-t)^{n-i} t^i \quad (2)$$

通常将折线  $P_0 P_1 \dots P_n$  看作是  $P(t)$  的控制多边形,将点  $P_0, P_1, \dots, P_n$  看作是  $P(t)$  的控制顶点。为了便于分析,下面重点研究一次 B-spline 曲线的图像融合。通过式 (1)、式 (2) 可得

$$P(t) = (1-t)P_0 + tP_1 \quad (3)$$

对于融合前的图像  $F_0$  与  $F_1$ , 假设其大小均为  $M \times N$ , 则有

$$F_0 = \{f_{ij}^0 | 0 \leq f_{ij}^0 \leq 255, 0 \leq i < M, 0 \leq j < N\} \quad (4)$$

$$F_1 = \{f_{ij}^1 | 0 \leq f_{ij}^1 \leq 255, 0 \leq i < M, 0 \leq j < N\} \quad (5)$$

对于  $F_0$  与  $F_1$  中同一位置的像素  $f_{ij}^0$  与  $f_{ij}^1$  有

$$f_{ij}^2 = (1-t)f_{ij}^0 + tf_{ij}^1, 0 \leq i < M, 0 \leq j < N \quad (6)$$

则融合图像可表示成

$$F_2 = \{f_{ij}^2 | 0 \leq f_{ij}^2 \leq 255, 0 \leq i < M, 0 \leq j < N\} \quad (7)$$

式中,  $x \rceil$  用于描述取不超过  $x$  的最大整数。依据式 (8)、式 (9) 可将融合前图像与加密图像从融合图像中分离出来

$$rf_{ij}^0 = \frac{f_{ij}^2 - tf_{ij}^1}{1-t}, 0 \leq i < M, 0 \leq j < N \quad (8)$$

$$rf_{ij}^1 = \frac{f_{ij}^2 - (1-t)f_{ij}^0}{t}, 0 \leq i < M, 0 \leq j < N \quad (9)$$

### 2.2 基于融合的军事图像加密通信中数据隐藏算法

基于融合的军事图像加密通信中数据隐藏算法能够融入所有形式的数据文件<sup>[7]</sup>, 数据文件以比特流的形式输入。假设串长为  $L$ , 将比特流分解成长为  $L$  的子串, 依据由上至下, 由左至右的顺序, 把子串排列成一个  $M \times N$  矩阵

$$S_{M \times N} = \begin{bmatrix} s_{11} & s_{12} & \dots & s_{1N} \\ \dots & \dots & \dots & \dots \\ s_{M1} & s_{M2} & \dots & s_{MN} \end{bmatrix} \quad (10)$$

其中  $s_{ij}$  表示长是  $L$  的比特子串, 同时其总长度不可超过  $M \times N \times L$ , 若超过则对其进行补“0”操作。假设一个  $M \times N$  矩

阵  $T_{M \times N}$  中的元素  $t_{ij}$  与  $S_{M \times N}$  中对应位置的比特子串十进制数值, 也就是

$$T_{M \times N} = \begin{bmatrix} t_{11} & t_{12} & \dots & t_{1N} \\ \dots & \dots & \dots & \dots \\ t_{M1} & t_{M2} & \dots & t_{MN} \end{bmatrix} \quad (11)$$

式中  $(t_{ij})_{10} = (s_{ij})_2$ , 当前  $T_{M \times N}$  的取值在  $[0, 2^L - 1]$  之间。假设  $f_{ij}^A = t_{ij} \times 2^{8-L}$ , 从而使建立的加密军事图像  $F_1$  的像素值保持在  $[0, 255]$ , 则加密军事图像  $F_1$  的像素值  $f_{ij}^A$  可表示成:  $\{f_{ij}^A | f_{ij}^A = i \times 2^{8-L}, i \in [0, 2^L - 1]\}$ 。

通过前文所述的基于融合的图像隐藏技术对数据进行融入操作。则对大小均为  $M \times N$  的原始加密军事图像  $F_0$  与  $F_1$  有

$$F_0 = \{f_{ij}^0 | 0 \leq f_{ij}^0 \leq 255, 0 \leq i < M, 0 \leq j < N\} \quad (12)$$

$$F_1 = \{f_{ij}^A | 0 \leq f_{ij}^A \leq 255, 0 \leq i < M, 0 \leq j < N\} \quad (13)$$

对式 (6) 进行调整, 使得数据融入与恢复过程中的误差相对降低, 则对于  $F_0$  与  $F_1$  中同一位置的各对像素  $f_{ij}^0$  与  $f_{ij}^A$  有

$$f_{ij}^2 = \text{round}(f_{ij}^0 \times (1-t)) + \text{round}(f_{ij}^A \times t) \quad (14)$$

通过式 (14) 可获取融合图像  $F_2 = \{f_{ij}^2 | 0 \leq f_{ij}^2 \leq 255, 0 \leq i < M, 0 \leq j < N\}$ , 其中  $\text{round}(x)$  用于描述与距离  $x$  最近的整数。

从融合图像中恢复军事图像加密通信中隐藏数据的过程即为融入隐藏数据的逆过程。首先将加密军事图像从融合图像中提取出来, 具体过程为

$$rf_{ij}^A = \text{round}((f_{ij}^2 - \text{round}((1-t) \times f_{ij}^0)) / t) \quad (15)$$

获取的加密军事图像为

$$rF_1 = \{rf_{ij}^A | 0 \leq rf_{ij}^A \leq 255, 0 \leq i < M, 0 \leq j < N\}$$

从加密军事图像中采集隐藏数据前, 需完成对加密军事图像误差的修正, 则有

$$rf_{ij}^{A'} = \begin{cases} rf_{ij}^A \ll (rf_{ij}^A \bmod 2^{8-L} \leq 2^{8-L-1} - 1) \\ rf_{ij}^A + 2^{8-L-1} - 1, \text{ otherwise} \end{cases} \quad (16)$$

经修正的像素值  $rf_{ij}^{A'}$  仍在  $[0, 255]$  之间。在修正的像素值  $rf_{ij}^{A'}$  中对其高  $L$  位比特进行采集, 即可获取  $rs_{ij}$

$$(rs_{ij})_2 = (rf_{ij}^{A'})_{10} = rf_{ij}^{A'} / 2^{8-L} \quad (17)$$

依据建立加密军事图像的逆过程即可获取所融入的比特流。在对军事图像加密通信中的数据进行隐藏的过程中, 数据融入方式是通过依据某种规律曲线的顺序扫描待隐藏数据的单元来实现的, 导致上述分析的基于融合的军事图像加密通信中数据隐藏算法, 由于检测工具有规律可循, 不容易逃脱检测, 无法对军事图像数据进行有效的隐藏。因此, 提出一种基于随机融入方式的不可逆数据隐藏算法。

## 3 随机融入方式的不可逆军事图像加密通信中数据隐藏算法

### 3.1 军事图像边缘特征

为了使隐藏容量和透明性之间实现最佳平衡, 需充分挖

掘军事图像视觉屏蔽特性。由于军事图像边缘是军事图像中最关键的结构信息之一,人眼对边缘信息相对较敏感,军事图像通信中数据的融入不应使军事图像边缘部分发生较大的变化,所以本文针对军事图像,直接提取军事图像边缘特征。由于军事图像较平滑区域的方差值较小,而边缘区域的方差值较大,因此可通过军事图像分块方差对其边缘特性进行刻画。分块 $B_{uv}$ 的方差 $\text{var}(u, v)$ 可通过以该分块为中心的邻域窗口 $W_{uv}$ 中每个分块 $DC$ 系数获取:

$$\text{var}(u, v) = \frac{1}{9} \sum_{(u', v') \in W_{uv}} (D(u', v') - \bar{D}(u', v'))^2 \quad (18)$$

式中 $\bar{D}(u', v')$ 用于描述以分块 $B_{uv}$ 为中心的邻域窗口 $W_{uv}$ 中的 $DC$ 系数平均值。

则各相邻 $DC$ 系数最大方差值可描述成:

$$\text{var}_{\max} = \left( \frac{D_{\max} - D_{\min}}{2} \right)^2 \quad (19)$$

通过式(18)、式(19)即可获取分块 $B_{uv}$ 的视觉敏感因子 $\lambda(u, v)$ :

$$\lambda(u, v) = \frac{\text{var}(u, v)}{\text{var}_{\max}} \quad (20)$$

因此给定阈值 $T$ ,如果 $\lambda(u, v) > T$ ,则相应军事图像分块 $B_{uv}$ 是军事图像边缘区域高频细节区,不允许其发生较大变化;否则,即为较平滑区域。在计算出军事图像边缘区域高频细节区后,应尽可能的避免这样的区域出现,以保证质量。

### 3.2 数据加密编码过程

数据加密编码过程是隐藏算法的关键一步,其过程如下:

输入:原始军事图像 $I$ ,密文序列 $w$ ,采样间隔 $\Delta u$ 与 $\Delta v$ ,融入等级 $L$ ,伪随机序列。

输出:载密军事图像 $\hat{I}$ ,关键编码信息 $O_{\text{info}}$ 。

1) 完成对原始军事图像 $I$ 的采样后,可获取一系列采样子图 $S_k(i, j)$ , $k = 1, \dots, \Delta u \times \Delta v$ ,从中找到一张参照军事子图 $S_{\text{ref}}$ ,塑造采样子图与参照子图间的军事差图 $E_k$ , $k = 1, 2, \dots, \text{ref} - 1, \text{ref} + 1, \dots, \Delta u \times \Delta v$ , $E_k$ 中的像素用 $e$ 描述。

2) 通过随机函数形成的伪随机序列完成对军事差图 $E_k$ 的置乱,获取的军事差图用 $E_{Rk}$ 进行描述, $E_{Rk}$ 中的像素用 $e_R$ 描述。

3) 建立所有 $E_{Rk}$ 的直方图 $H_{Rk}$ ,通过融入等级 $L$ 对直方图 $H_{Rk}$ 进行平移,得到的军事差图中的像素 $e_R$ 可表示为

$$\hat{e}_R = \begin{cases} e_R + L + 1 & e_R > L \\ e_R - L - 1 & e_R > -L \\ e_R & \text{其他} \end{cases} \quad (21)$$

4) 对所有像素 $\hat{e}_R$ 进行扫描,按照融入等级,在像素值 $[-L, L]$ 间融入数据 $w$ , $w \in [0, 1]$ 。隐藏数据后的像素 $\hat{e}_{RW}$ 可

通过式(22)获取,隐藏数据后的军事差图用 $\hat{E}_{RW}$ 描述。

$$\hat{e}_{RW} = \begin{cases} 2L + w & \hat{e}_R = L \\ -2L - w & \hat{e}_R = -L \\ \hat{e}_R & \text{其他} \end{cases} \quad (22)$$

5) 依据步骤2)中数组 $X_k$ 下标和像素位置关系,对所有军事差图 $\hat{E}_{RW}$ 中的像素的位置进行恢复,获取融入信息的军事差图 $\hat{E}_{kW}$ ,通过参照子图获取融入信息的子图 $S_{kW}$ 。

6) 完成参照子图 $S_{\text{ref}}$ 与嵌有信息子图 $S_{kW}$ 的逆采样,获取密图 $\hat{I}$ , $\Delta u, \Delta v, L$ 和 $X_k$ 等,将其作为关键编码信息 $O_{\text{info}}$ 进行输出。

### 3.3 数据解压与军事图像恢复过程

数据隐藏的提取方法即数据融入的逆过程,主要通过下述步骤实现:

1) 将隐藏数据合成相应的数据隐藏码流(以遭受攻击时提取 $8 - \text{bits}$ 数据为例):

$$W^*(u, v) = W_{b1}^*(m, n) + W_{b2}^*(m, n) + \dots + W_{b8}^*(m, n) \quad (23)$$

2) 完成所有军事差图的置乱操作,经置乱后的数据格式可通过下式获取:

$$W^*(u, v) = \begin{cases} 1 & \sum_{k=1}^M W_{bk}^*(m, n) \geq 0 \\ -1 & \text{其他} \end{cases} \quad (24)$$

3) 将置乱后的军事差图中得隐藏数据按照数据隐藏的正确率进行度量,实现军事图像加密通信中的数据隐藏:

$$BCR = \frac{\sum_{m=1}^M \sum_{n=1}^N \overline{W(u, v) \oplus W^*(u, v)}}{U \times V} \quad (25)$$

## 4 实验分析

为了验证本文方法的有效性,需要进行相关的实验分析。本实验在MATLAB 7.0环境下对加密通信中的军事图像进行编码获取测试图像,以峰值信噪比PSNR为评价标准实现对加密军事图像质量的评价。

图1描述的是原始军事图像,图2、图3分别描述了本文方法和传统方法的数据隐藏效果图。分析图1、图2与图3可以看出,采用本文方法获取的数据隐藏效果图明显优于传统方法,验证了本文方法的有效性。

表1描述的是本文方法和传统方法隐藏容量的比较。从表1可以看出,与传统方法相比,本文方法具有良好的隐藏容量,也就是PSNR性能。

表1 本文方法和传统方法隐藏容量比较

方法	隐藏容量/bit	军事图像文件 大小/Byte	PSNR/dB
传统方法	53842	53314	38.1275
本文方法	65149	52517	39.3497



图1 原始军事图像



图2 传统方法军事图像数据隐藏算法



图3 本文方法军事图像数据隐藏算法

为了进一步验证本文方法的性能,图4给出了不同融入率下,本文方法和传统方法军事图像加密通信中数据隐藏算法的隐秘图像PSNR测试结果。从图4可以看出,在融入相同军事图像加密通信中的数据时,本文方法生成的加密军事图像具有更好的视觉质量,人眼很难看出隐藏数据的存在。

## 5 结论

本文提出一种采用随机融入方式的不可逆数据隐藏算法,直接提取军事图像边缘特征,充分挖掘军事图像视觉屏蔽特性,通过军事图像分块方差对其边缘特性进行刻画,确保军事图像边缘的完整度,构建军事图像采样子图与参照子图间的军事差图,通过数据隐藏的提取方法,将隐藏军事图像差图数据合成相应的数据隐藏码流,完成所有军事差图的置乱

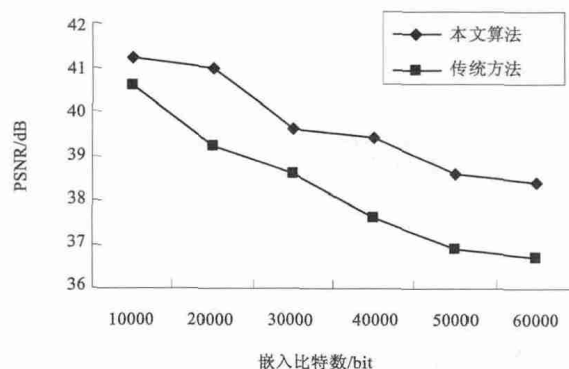


图4 本文方法与传统方法的透明性比较

操作,将置乱后的军事差图中的隐藏数据按照数据隐藏的正确率进行度量,实现军事图像加密通信中的数据隐藏。仿真结果表明,采用所提方法对军事图像加密通信中的数据进行隐藏的效果与隐藏容量均优于传统方法,验证了所提方法的有效性。

## 参考文献:

- [1] 王建军,王颖. 一种基于K-Fibonacci矩阵和JPEG的数据隐藏方法[J]. 系统工程与电子技术, 2006, 28(8): 1252-1257.
- [2] 白建荣,贾永红,潘鹏. 一种修改JPEG图像量化表的信息隐藏方法[J]. 武汉大学学报:信息科学版, 2009, 34(10): 1236-1239.
- [3] 邱应强,等. 一种基于JPEG压缩图像的信息隐藏方法[J]. 电路与系统, 2008, 13(5): 129-135.
- [4] 刘光杰,等. 用于JPEG图像的高容量信息隐藏算法[J]. 信息与控制, 2007, 36(1): 102-107.
- [5] 熊志勇,高志荣,姜卓睿. 基于整数小波变换和差值扩展的可逆数据隐藏[J]. 中南民族大学学报(自然科学版), 2010, 29(3): 68-74.
- [6] 柳葆芳,平西建,邓宇虹. 基于融合的数据隐藏算法[J]. 电子学报, 2001, 11(02): 44-46.
- [7] 柳玲,陈同孝,曹晨等. 一种随机嵌入抗SPAM检测的可逆数据隐藏算法[J]. 计算机应用研究, 2013, 30(07): 2111-2114.



## 【作者简介】

岳鑫(1990-),男(汉族),四川南充人,在读硕士研究生,主要研究方向为信息安全;

周城(1963-),男(汉族),江苏无锡人,硕士,硕士研究生导师,副教授,主要研究方向为信息安全、密码学;

甘文道(1990-),男(汉族),云南楚雄人,在读硕士研究生,主要研究方向为信息安全;

张铭隆(1989-),男(汉族),四川内江人,在读硕士研究生,主要研究方向为图像处理。