一种新型的信息隐藏方法及其硬件实现

邓 攀[1],苗 鑫[1],张晶如[1],殷 奕[2],唐 燕[3]

(1. 南京师范大学物理科学与技术学院,江苏 南京 210023)
(2. 南京师范大学计算机科学与技术学院,江苏 南京 210023)
(3. 南京师范大学地理科学学院,江苏 南京 210023)

[**摘要**] 提出了一种基于规范类正交矩阵的信息隐藏及提取电路的设计与 FPGA 实现. 利用基于构造矩阵的查找算法和克罗内克积扩展,实现规范类正交矩阵快速构造;隐秘数据经过规范类正交矩阵编码后,具备线性性质,修正相关检测后的判决输入数据,实现隐秘数据的提取;鉴于多媒体数据处理的速度和嵌入隐秘信息的效率要求,采取了使用 FPGA 实现基于规范类正交矩阵的信息隐藏及提取电路的设计方案. 结果表明,该装置电路结构简单,能够满足多媒体数据实时处理的要求;在发送端,隐秘信息被快速嵌入到载体数据流中;在接收端,通过生成相同的规范类正交矩阵,分别将载体信息和隐藏信息准确地提取出来.

[**关键词**] 规范类正交矩阵,信息隐藏,现场可编辑门阵列
[**中图分类号**]TN47 [**文献标志码**]A [**文章编号**]1672-1292(2013)01-0055-07

A Novel Information Hiding Algorithm and its Hardware Implementation

Deng Pan[1], Miao Xin[1], Zhang Jingru[1], Yin Yi[2], Tang Yan[3]

(1. School of Physics and Technology, Nanjing Normal University, Nanjing 210023, China)
(2. School of Computer Science and Technology, Nanjing Normal University, Nanjing 210023, China)
(3. School of Geographical Science, Nanjing Normal University, Nanjing 210023, China)

Abstract: This paper presents information hide based on specification class orthogonal matrix and extraction circuit design and FPGA implementation. It uses the search algorithm based on the structural matrix and the Kronecker product expansion to realize the rapid construction of the normal similar-orthogonal matrix. The hidden data after the normal similar-orthogonal matrix coding, has a linear nature. The judgement after the revised relevant detections is taken as input data to realize the extraction of the hidden data. In view of multimedia data processing speed and efficiency of embedding secret information requirements, FPGA is used to realize a design program of hidding information based on the normal similar-orthogonal matrix, and extracting circuits. The results show that the apparatus circuit configuration is simple, and can meet the requirements of real-time processing of the multimedia data. And that at the transmitting end, the secret information is embedded fast to the carrier in the data stream by generating the same canonical class orthogonal matrices, and that at the receiving end, the carrier information and hidden information are accurately extracted.

Key words: normal similar-orthogonal matrices, information hiding algorithm, FPGA

信息隐藏技术是利用人类感官的不敏感性和信息本身存在的冗余,采用软件或硬件的方法将某种信息嵌入到宿主信号(如图像、声音、视频或文本文档)中,并在必要时可检测或提取隐藏信号的技术. 对于隐藏算法,一方面需要增加分析复杂度,提高算法安全性. 另一方面,对隐体的提取应该是不需要原始载体或原始隐体. 而将扩频技术应用到信息隐藏领域中,可显著增强系统的鲁棒性和安全性. 扩频隐藏算法多采用 CDMA 中的正交扩频码,如 Hadamard 码、Walsh 码、Gold 码或 m 序列等[1-3]. 信息隐藏的系统框图如图 1 所示.

扩频隐藏算法是通过一个序列或多个序列,将原始隐秘数据进行扩频编码,即用扩频序列加密原始隐秘数据. 基于这个思想,定义了一种规范类正交(Normal Similar-orthogonal, NS)矩阵,该矩阵中任意两行的互相

收稿日期:2012-12-10.
基金项目:国家自然科学基金(2008105GZ30031)、江苏省高校自然科学基金(2010119TSJ0119).
通讯联系人:殷奎喜,教授,博士生导师,研究方向:移动通信、电子信息处理. E-mail:yinkuixi@njnu.edu.cn

关系数为定值. 秘密信息经 NS 矩阵编码后,得到加密的数据,再嵌入到载体中,提高了隐秘数据的安全性. 在接收端,不需要原始载体图像,仅使用相同 NS 矩阵,即可恢复出原始秘密信[4,5].

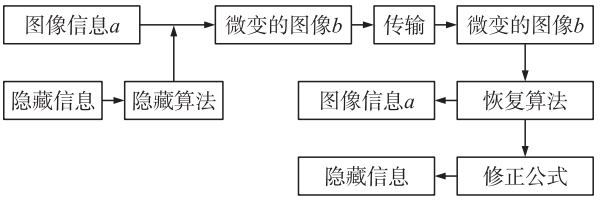

图 1　隐藏方法系统框架图

Fig. 1　Method of hiding the system frame diagram

通常软件实现的信息隐藏系统速度较慢,不能满足多媒体数据实时处理的要求,为了达到高速处理的性能要求,采用硬件实现信息隐藏算法具有很重要的意义. FPGA 作为一种最具代表性的 PLD 器件,继承了 ASIC 的大规模、高集成度、高可靠性的优点,又克服了普通 ASIC 设计周期长、投资大、灵活性差的缺点. 随着工艺技术的发展和市场需要,超大规模、高速、低功耗的新型 FPGA 器件不断推陈出新. 新一代的 FPGA 甚至集成了 CPU 或 DSP 内核,在一片 FPGA 上进行软硬件协同设计,为实现 SOPC 提供了强大的支持. 无论是在速度、体积,还是在设计的灵活性上,FPGA 都能适应图像和信号处理的要求.

1　信息隐藏与提取方法

1.1　规范类正交矩阵

定义 $L\times N$ 规范类正交矩阵 $\boldsymbol{K}$ 中任意一个元素 $k_{ij}\in\{-1,+1\}$ $(i=1,2,\cdots,L;j=1,2,\cdots,N;L\leqslant N)$;$\boldsymbol{K}$ 中任意两行之间的互相关系数 $\rho_{it}=\dfrac{p}{N}$(p 为定值;$p\in\{-N+2,-N+4,\cdots,N-2\}$;$t=1,2,\cdots,L$).

规范类正交矩阵的构成方法如下:

(1)当码长为 N 时,二进制完备码组数为 $L=2^N$,$\boldsymbol{x}_t$ 表示任意码组,其中 $t\in\{0,1,\cdots,2^N-1\}$ 为该二进制码对应的十进制编号.

(2)定义构造矩阵 $\boldsymbol{P}$ 中任意元素 $\rho_{ij}=<x_i,x_j>$,可见构造矩阵 $\boldsymbol{P}$ 包含了所有码组的互相关信息,N 值一定时,构造矩阵唯一.

(3)定义编号集合 $Path=\{a_1,a_2,\cdots,a_M\}$,其中 $a_1,a_2,\cdots,a_M\in\{0,1,\cdots,2^N-1\}$,则 x_{a_t} 表示编号 a_t 对应的码组.

(4)输入参数包括构造矩阵 $\boldsymbol{P}$,码组长度 N,初始编号 a_1,互相关系数 p;输出参数包括规范类正交矩阵 $\boldsymbol{K}$,规范类正交矩阵行数 M;查找规则从左向右、从上到下.

(5)利用构造矩阵实现规范类正交矩阵构造的算法如下:

1)初始化. $Path=\{a_1\}$,$M=1$,行号 $i=a_1$,列号 $j=a_1$.

2)如果 $j=L$,转至步骤 5). (步骤 5 牵涉到已申请的专利在此不予给出).

3)如果 $\rho_{ij}\neq p$,$j=j+1$,返回步骤 2).

4)如果对每个 $t\in Path$ 都满足 $\rho_{jt}=p$,增加编号至集合 $Path=Path\cup\{i\}$,$M=M+1$,$i=j$,转至步骤 2);否则直接返回步骤 2).

输出 $\boldsymbol{K}=(\boldsymbol{x}_{a_1}\quad\boldsymbol{x}_{a_2}\quad\cdots\quad\boldsymbol{x}_{a_M})^{\mathrm{T}}$.

1.2　信息隐藏与提取

设隐秘信息 $\boldsymbol{B}=(b_1,b_2,\cdots,b_L)$,$b_i\in\{-1,+1\}$,"-1"表示二进制"0","+1"表示二进制"1". 则其经 NS 矩阵的加密过程为 $\boldsymbol{W}=\boldsymbol{BK}$,其中,$\boldsymbol{W}=\{w_1,w_2,\cdots,w_N\}$ 为加密信息. 实际隐藏点的载体数据为 $\boldsymbol{X}=(x_1,x_2,\cdots,x_N)$;含密载体数据 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_N)$,嵌入强度 $\boldsymbol{G}=(g_1,g_2,\cdots,g_N)$,则嵌入函数 $\boldsymbol{Y}=\boldsymbol{X}+\boldsymbol{G}\odot\boldsymbol{W}$(符号 $\odot$ 表示 Hadamard 积,也称 Schur 积).

信号经过信道时受到干扰或攻击为 $\boldsymbol{E}=(e_1,e_2,\cdots,e_N)$,接收端得到的数据为 $\boldsymbol{Z}=\boldsymbol{Y}+\boldsymbol{E}$,相关检测矩阵 $\boldsymbol{K}^{\mathrm{T}}$,使用相关检测法,得到判决输入数据 $\boldsymbol{r}=\boldsymbol{ZK}^{\mathrm{T}}=\boldsymbol{XK}^{\mathrm{T}}+\boldsymbol{G}\odot\boldsymbol{S}+\boldsymbol{EK}^{\mathrm{T}}$($\boldsymbol{r}=(r_1,r_2,\cdots,r_L)$).

各个判决输入数据为 $r_i=\sum\limits_{j=1}^{N}x_jk_{ij}+\sum\limits_{j=1}^{N}\left(\sum\limits_{t=1}^{L}g_tb_ik_{ti}\right)k_{ij}+\sum\limits_{j=1}^{N}e_jk_{ij}$. 则判决输入数据修正为 $R_i=r_i-\dfrac{p}{[N+(L-1)p]}\sum\limits_{t=1}^{L}r_t$.

判决规则为,若 $R_i>R_0$,则判为“1”;若 $R_i<R_0$,则判为“0”;其中,R_0 为判决门限.

2　FPGA 实现

2.1　二维 DCT 的实现

为保证数据隐藏过程的可靠性和保密性,本文将经规范类正交矩阵编码的隐秘数据嵌入到图像的 DCT 域,所涉及的图像的二维 DCT 变换的具体实现方法如下[6-8]:

假定图像的像素块大小为 $N\times N$,若令图像单位素点的数据为 $x(i,j)$,则其二维 DCT 变换为:

$$Z(u,v)=\frac{2}{N}C(u)C(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}x(i,j)\cos\left(\frac{(2i+1)u\pi}{2N}\right)\cos\left(\frac{(2j+1)v\pi}{2N}\right);$$

其中,$u,v=0,1,\cdots,N-1$;$C(u),C(v)=\begin{cases}\frac{1}{\sqrt{2}} & u,v=0\\ 1 & u,v\neq 0\end{cases}$.

上式可以修改为:

$$Z(u,v)=\sqrt{\frac{2}{N}}C(u)\sum_{i=0}^{N-1}\left[\sqrt{\frac{2}{N}}C(v)\sum_{j=0}^{N-1}x(i,j)\cos\left(\frac{(2j+1)v\pi}{2N}\right)\right]\cos\left(\frac{(2i+1)u\pi}{2N}\right).$$

令
$$Y(a,b)=\sqrt{\frac{2}{N}}C(v)\sum_{j=0}^{N-1}x(i,j)\cos\left(\frac{(2j+1)v\pi}{2N}\right);$$

则
$$Z(u,v)=\sqrt{\frac{2}{N}}C(u)\sum_{i=0}^{N-1}Y(a,b)\cos\left(\frac{(2i+1)u\pi}{2N}\right).$$

从以上两式不难看出,二维 DCT 可以由 2 个一维 DCT 组合构成. 简记 $\boldsymbol{Z}=\boldsymbol{CXC}^{\mathrm{T}}$,其中,$\boldsymbol{C}$ 为余弦变换系数矩阵. 于是,$\boldsymbol{Y}=\boldsymbol{XC}^{\mathrm{T}}$,$\boldsymbol{Z}=\boldsymbol{CY}$. 对于 $N\times N$ 的系数变换矩阵 $\boldsymbol{C}_{ij}=\sqrt{\frac{2}{N}}\cos\left(\frac{(2j+1)i\pi}{2N}\right)$,若采用的是 2×2 的 DCT 块,则其变换矩阵 $\boldsymbol{C}=\begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \cos\frac{\pi}{4} & \cos\frac{3\pi}{4}\end{bmatrix}$.

二维 DCT 的实现是通过二次一维 DCT 的变换得到的,实现流程如图 2 所示. 本文采用的是 2×2 的 DCT 块. 之所以采用 2×2,是因为本文牵涉的信息隐藏需要进行替换,2×2 的矩阵具有较好的相似性,对图像进行如此处理,就不容易察觉,图像隐藏了相关性,且在后续编程中,可以此模块进行拓展.

图 2　二维 DCT 处理流程

Fig. 2　Two dimensional DCT process

对于 1 个 2×2 的数据块来说,共有 4 个数据,以串行的方式输入,可将这 4 个数据分组,每行数据为一组,共 2 组. 当第一组数据输入后,经串并电路将其变为并行数据,而后经过一维 DCT 的变换电路完成 1 行数据的 DCT 变换,再通过并串电路将数据串行存入 RAM 中. 当所有行数据完成一维 DCT 变换并存储完毕后,经转置将其从 RAM 中取出,再经串并电路送入后一个 DCT 变换电路,按列进行一维 DCT 变换. 完成一列的一维 DCT 变换后,再经过串并电路将数据输出[9,10]. 所有数据完成转换后,即形成了一个 2×2 数据块的二维 DCT 变换. 2×2 数据块的二维 DCT 其实并非需要如此多步骤,而本文之所有进行化简为繁进行操作处理,是因为此二维 DCT 硬件实现方法是目前较主流的硬件实现方式,在此基础上很容易进行延伸的变换. 二维 DCT 的实现难点是如何实现一维 DCT,而一维 DCT 算法需要多个乘法器,用硬件实现会占用大量资源,且多位的乘法器处理速度也非常低,故本文将固定系数预先放在查找表中,将乘法运算转换为移位求和实现,结果如图 3 所示. 因为 DCT 变换会出现负数,所以本文设计的加法器是有符号位的加法器,而对于可能出现的溢出,采用多保留一位,于是同号加时(即正+正或者负+负),可以避免让可能出现的进位影响到符号位. 而对于在

DCT 变换中出现的乘法器的设计,采用的是移位来实现乘法,如移动 10 位,即先扩大 1 024 倍,待计算结束后再缩小 1 024 倍,这样便解决了 DCT 运算中出现的余弦函数表的问题.

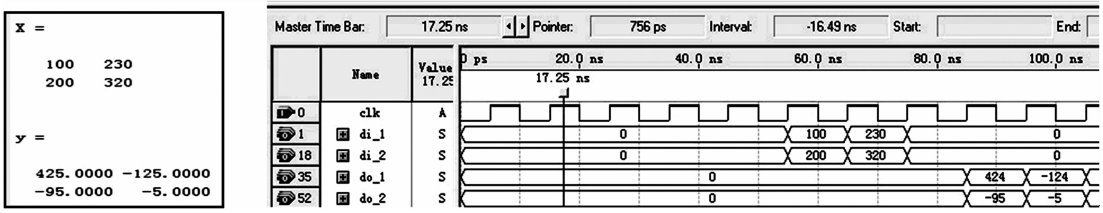

图 3　Matlab 和 Quartus 上实现的 2×2 DCT 子模块

Fig. 3　Matlab and Quartus on the realization of the 2× 2 DCT module

2.2　5 个重要模块

信息的隐藏及隐藏信息的提取主要由 5 个模块组成:(1)秘密数据和矩阵控制模块;(2)秘密数据、控制矩阵保存和相乘模块;(3)控制模块;(4)信息隐藏实现模块;(5)隐藏信息提取模块.

2.2.1　秘密数据和矩阵控制模块

秘密数据和矩阵控制模块用以输入秘密数据和控制矩阵. 当需要重新输入矩阵元素值的时候将矩阵复位信号置低一个时钟信号,而矩阵数据则采用按行输入. 另外矩阵和秘密数据的输入应尽量在 DCT 转换数据的输入之前,因为 DCT 转换是顺序转换的,若在 DCT 转换时矩阵和秘密数据还未输入进系统,则 DCT 转换后的数据就会不准确. 在程序的编写中,还定义计数值 count,用以控制每次输入的秘密数字及控制矩阵的一行. 对于矩阵数据,本文放大了 256 倍,待计算完成后,会除去 256 倍还原.

2.2.2　秘密数据、控制矩阵保存和相乘模块

秘密数据、控制矩阵保存和相乘模块是接在秘密数据和矩阵控制模块后的,故此模块的输入为上一模块的输出,此模块计算出秘密数据和控制矩阵相乘的结果也即 $\boldsymbol{W}_n$. 为实现矩阵与向量相乘,还建立了子模块 MatrixMuxVector8,需注意的是,之前曾将数据放大 256 倍,则在此模块中,去除结果的后 8 位,缩小 256 倍. 由于此处出现的值均为 2 的幂次,故在这些模块的编写中,使用加法器的移位实现乘法,可有效节约硬件资源. 而在 DCT 和 iDCT 的程序编写中,则不可通过该方法实现乘法器,故调用系统的 IP 核实现乘法.

2.2.3　控制模块

控制模块参照此模块里面的时序来使用后面的变换模块. 此模块的作用是发送矩阵,每组矩阵中包含了 4 个 2×2 的小矩阵块,这些矩阵块是用以后续进行 DCT 变换等一系列处理的.

2.2.4　信息隐藏实现模块及实现方法

信息隐藏实现模块 DCT 模块的作用,是将之前的原始数据进行细化分析处理并实现将秘密数据变为一个微量隐藏到矩阵中,如图 4 所示. n 位二进制秘密数据与 $n\times n$ 的 $\boldsymbol{K}$ 矩阵相乘后,会得到 n 个数据 W_1, $W_2\cdots W_n$,这些数据将秘密数据隐含其中,通过图中的计算公式将其作为一个微量隐藏在经过 2×2 分块

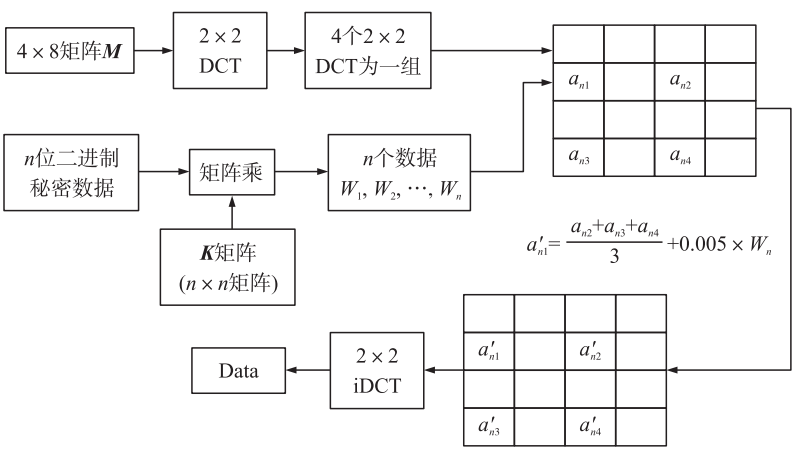

图 4　隐藏信息的发送流程示意图

Fig. 4　The hidden information transmitting process sketch map

DCT 变换的一个数组中,再对这个隐藏了秘密数据的数组进行 2×2 分块的 iDCT 变换,得到的数据便是隐藏了秘密信息的数据 data.

信息隐藏模块主要由以下模块构成:

(1)接收数据模块. 其主要功能是将串行接收到的数据按 4 个 2×2 矩阵分为一组,分 8 组顺次从输出端口输出. 供其后的 DCT(和 IDCT)变换模块进行变换,每一组变换有 holder 信号触发,转换完成由信号 holder1 触发.

(2)数据保持模块. 其作用是 clk 端每来一个脉冲,该模块便将输入端口复制给输出端口一次,这样可保证其后每一次 DCT 转换过程中该端口的值保持恒定.

(3)二维 DCT 变换模块(2×2). 此模块利用快速二维 DCT 变换方法进行二维 2×2 的 DCT 变换. 其变换方法可以简述如下:设一维 DCT 变换矩阵为 $\boldsymbol{Y}=\boldsymbol{CX}$,$\boldsymbol{C}$ 为变换矩阵,则二维 DCT 变换可简述为 $\boldsymbol{Z}=\boldsymbol{C}\times\boldsymbol{C}'$. 即令 $\boldsymbol{Y}=\boldsymbol{XC}'$,则 $\boldsymbol{Z}=\boldsymbol{CY}$. ($\boldsymbol{C}'$为 $\boldsymbol{C}$ 的转置),此处共需 4 个此模块.

(4)隐藏变换模块. 该模块的作用是计算隐藏了秘密数据的图像矩阵中的某一个特定位置的值. 输出 an1 即为变换过后的新的 an1 值. 在程序编写中,运用了防溢出的方法进行处理.

对矩阵进行过 dct 变换并进行信息隐藏处理后,还需进行 dct 逆变换,iDct2 模块便是实现此功能的模块. 此时需要 4 个 iDCT 变换模块与之前的 4 个 DCT 模块进行对应. 经过如此处理以后,图像只会发生微变,但秘密数据已隐藏其中. Matlab 仿真如图 5 所示.

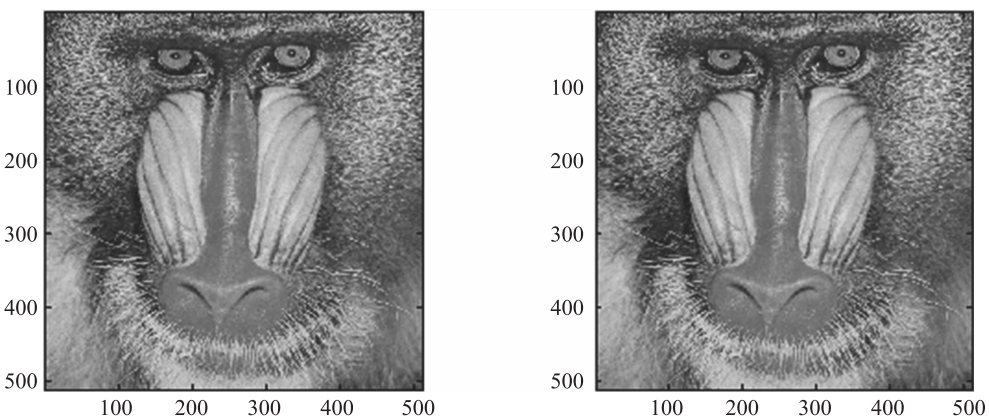

图 5　原始及隐藏信息图

Fig. 5　The original and the hidden information graph

此外还有延时模块 Delay、输出使能计数器模块 count 和秘密数据选择模块 dctsecnum 等,此处不再赘述.

2.2.5　隐藏信息提取模块和实现方法

隐藏信息的提取只需对加密过程进行逆向并进行一定的修正即可. 在接收到信息隐藏发送模块发送来的 Data 后,需对其进行 2×2 分块 DCT,以此来得到包含了隐藏信息的 a'_{n1}. 此后再进行与矩阵 $\boldsymbol{K}$ 的转置乘,得出结果 R_n. 此时的 R_n 即包含了所需的秘密数据,但并非最终结果,还需进行修正,修正的方法如 1.2 节所述,具体修正公式因申请专利不予给出. 最终得出的修正结果,便为最终隐藏的秘密数据. 具体流程如图 6 所示.

隐藏信息提取模块主要由以下模块构成:

(1)获取 an1 模块. 其功能是将每一小组转换后的 an1 保存并从输出端口输出.

(2)除法模块 div3 模块. 其作用是求出 an1 = (an2+an3+an4)/3.

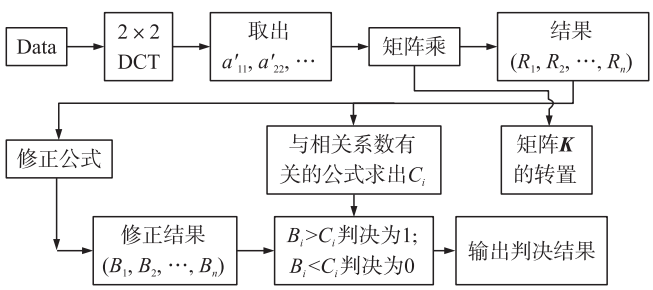

图 6　隐藏信息的解码过程

Fig. 6　The hidden information in the decoding process

(3)Add8num2 模块. 其功能是数据相加的模块;Div9 模块,除以 9 的除法模块;Calbi 模块,其本质是一个减法器模块;通过以上 3 个模块结合求出修正结果 B_i,C_i.

(4)比较判决模块 Verify,将 B_i,C_i 进行判决并最终得出判决输出.

3　功能验证及性能分析

本实施例在 Altera 公司集成设计环境 Quartus 下,选用 Cyclone Ⅲ 的 EP3C80G780C6 器件实现综合与仿真. 整个电路采用 verilog HDL 语言描述,图像数据由矩阵构成,为较直观的验证结果,采用 8 组 4×8 的矩阵,给出了一组 8 位秘密二进制数据,8 位二进制值为 1、-1、1、-1、-1、-1、-1、1,要求将秘密数据隐藏在图像中.

由图 7 看出,本程序占用了 15 533 个逻辑单元,硬件利用率为 19%;52 个管脚,应用利用率为 12%;464 个乘法器单元,硬件资源利用率为 95%. 由图 8 可见,在 Quartus 硬件平台上成功地提取了隐藏的信息.

Flow Status	Successful-Wed Aug 15 20:17:14 2012
Quartus II Version	9.0 Build 235 06/17/2009 SP 2 SJ Web Edition
Revision Name	mdct
Top-level Entity Name	mdct
Family	Cyclone III
Device	EP3C80F780C6
Timing Models	Final
Met timing requirements	N/A
Total logic elements	15 533 / 81 264(19%)
Total combinational functions	14 949 / 81 264(18%)
Dedicated logic registers	1 412 / 81 264(2%)
Total registers	1 412
Total pins	52 / 430(12%)
Total virtual pins	0
Total memory bits	0 / 2 810 880(0%)
Embedded Multiplier 9-bit elements	464 / 488(95%)
Total PLLs	0 / 4(0%)

图 7　综合编译时显示的器件资源使用情况

Fig. 7　Display integrated compile-time device resource usage

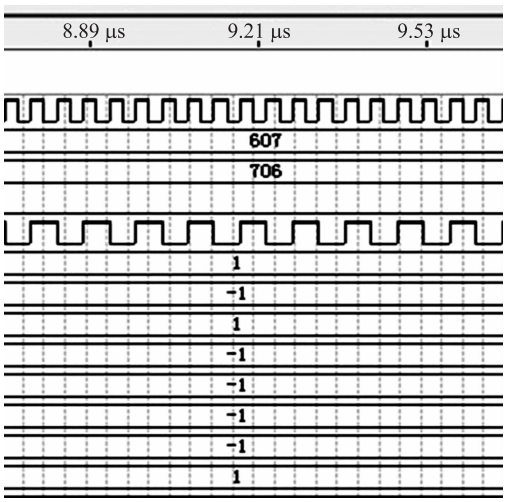

图 8　整体模块仿真时序图

Fig. 8　Module simulation timing diagram

本文采用 2×2 分块 DCT 的重要原因,见图 9 和图 10 的黑框,同样的输入,在 Matlab 运算输出 y 的第一行第一列为 309.3750 为准确值,而在图 10 中相同值则变为 307,可见 8×8 的分块 DCT 比 2×2 的分块 DCT 对结果的影响更大,且 2×2 的 DCT 更适合所选的 $a_{nm}(m=1,2,3,4)$.

Command Window

New to MATLAB? Watch this Video, see Demos, or read Getting Started.

image =

0	0	0	0	0	0	0	0
32	12	12	12	65	12	-12	-52
36	36	15	36	36	12	-36	-36
38	98	56	98	35	25	-12	-98
69	125	126	125	56	25	0	-125
95	136	136	136	98	18	-8	-136
126	145	145	145	126	16	-25	-145
65	198	156	198	255	8	-36	-198

y =

309.375 0	400.874 5	-295.349 2	53.913 0	-36.375 0	0.352 2	-95.358 5	21.020 3
-220.920 6	-254.778 7	199.909 3	-2.894 5	25.279 5	3.753 1	76.963 2	-32.478 6
3.522 6	-19.622 3	-35.584 1	15.429 4	42.280 7	-44.696 2	-18.246 8	52.528 8
1.639 3	-4.199 1	50.497 3	-21.870 8	-30.087 3	46.028 7	25.759 2	-1.446 5
12.375 0	2.797 3	-39.629 6	-23.763 2	-26.375 0	-5.142 7	-34.592 6	-15.936 6
-21.708 9	-13.720 7	50.030 5	-11.643 7	2.839 1	14.351 9	18.012 4	-29.787 9
-6.194 6	-14.380 4	-3.496 8	-15.171 0	8.328 9	-16.392 8	-6.415 9	-5.203 1
-5.239 1	-4.151 1	26.802 4	-11.664 2	3.931 0	5.272 7	22.004 4	-2.7024

fx >>

图 9　Matlab 上 8×8 分块 DCT 的输入(图中 image)及输出(图中 y)

Fig. 9　The Matlab 8 ×8 DCT block input(image) and output(y)

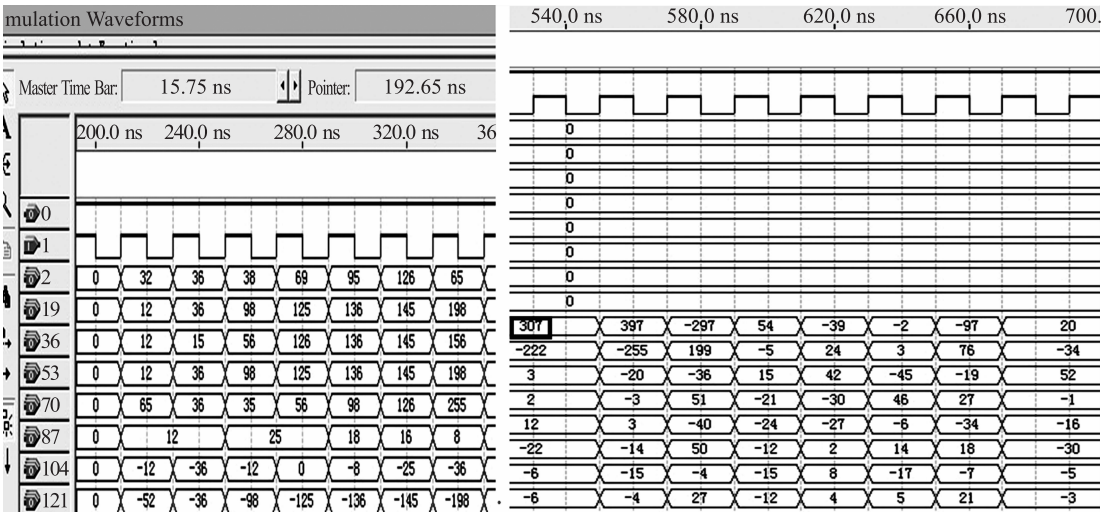

图 10　Quartus 上 8×8 分块 DCT 的输入(左)及输出(右)

Fig. 10　The Quartus 8×8 DCT block input(left) and output(right)

4　结语

此前的各种信息隐藏,基本只可在计算机上仿真验证,实际应用有限. 本文所述新型的信息隐藏方式,不仅在理论上可行,且可在硬件上成功实现,目前已做到一次处理 8 位数据. 由于是以 2×2 为子 DCT 模块,所以易继续拓展至 16 位、32 位运算,运用前景巨大,且一次运算所需时间极短,不到 9 μs. 但 8 位运算时,已经使用了 95% 的乘法器资源,为节约成本,下一步将努力优化程序,更充分地利用硬件资源.

[参考文献](References)

[1] 陈伟超,敖珺马,马春波. 基于 DCT 特性的图像隐藏稳健扩频算法[J]. 计算机工程,2011,37(10):55-60.
Chen Weichao,Ao Junma,Ma Chunbo. Based on the characteristics of DCT image hiding algorithm of robust spread spectrum[J]. Computer Engineering,2011,37(10):55-60. (in Chinese)

[2] Celik M,Sharma G,Tekalp,et al. Lossless generalized-LSB data embedding[J]. IEEE Transaction on Image Processing,2005,14(2):253-266.

[3] Ker A. Steganalysis of LSB matching in grayscale images[J]. IEEE Signal Processing Letters,2005,12(6):441-444.

[4] 邵菲,花俊. 基于 Walsh 序列扩频的图像信息隐藏[J]. 理论与方法,2009,29(8):71-77.
Shao Fei,Hua Jun. Based on the Walsh sequence spread spectrum image information hiding[J]. Theory and Method,2009,29(8):71-77. (in Chinese)

[5] 高琦,李人厚,王慧琴,等. 基于 Gold 码的扩频数字水印算法[J]. 西安交通大学学报,2004,38(2):68-75.
Gao Qi,Li Renhou,Wang Huiqin,et al. Based on the gold code spread spectrum digital watermarking algorithm[J]. Journal of Xi'an Jiao Tong University,2004,38(2):68-75. (in Chinese)

[6] Bansal A,Bhadouria S. Network security and confidentiality with digital ateim arking[C]//Proceedings of 2007 Digatal E co-Systems and Technologies Conference. Inaugural:IEEE-IES,2007:25-328.

[7] 何云壮,刘永强,李勇权. H.264 整数 DCT 的 FPGA 实现[J]. 微计算机信息,2007,23(17):86-93.
He Yunzhuang,Liu Yongqiang,Li Yongquan. H.264 integer DCT FPGA implementation[J]. Micro Computer Information,2007,23(17):86-93. (in Chinese)

[8] 李莉,宁帆,魏巨升. 基于 DA 算法的二维 DCT 的 FPGA 实现[J]. 现代电子技术,2006,225(10):44-49.
Li Li,Ning Fan,Wei Jusheng. DA algorithm based on two dimensional DCT FPGA implementation[J]. Modern Electronic Technology,2006,225(10):44-49. (in Chinese)

[9] 孙中,许刚. 一种基于 α 稳定分布模型的 DCT 域隐藏信息检测新方法[J]. 电子学报,2008,36(4):45-53.
Sun Zhong,Xu Gang. A method based on the alpha stable distribution model of DCT domain information hiding detection method[J]. Chinese Journal of Electronics,2008,36(4):45-53. (in Chinese)

[10] Kuruoglu E E,Fitzgerald P W J,Rayner W J. Near optimal detection of signals in impulsive noise modeled with a sym-metric stable distribution[J]. IEEE Communications Letter,1988,2(10):282-285.

[责任编辑:严海琳]