短公钥的可证明安全基于身份数字签名算法

王之怡[1] 刘 铁[2] 康 立[1] 谢 静[1] 雷 刚[1]
(西南财经大学经济信息工程学院 成都 610074)[1] (IBM中国研究院 北京 100193)[2]

摘 要 在标准模型下的适应性选择消息不可伪造攻击(UCMA)安全模型中,Paterson和Schuldt(PS)构造了双线性映射群中基于计算DH难题的基于身份数字签名算法。PS算法直接利用两组独立的Waters身份处理函数去分别处理用户身份和签名消息,因此算法中公钥参数数量很大。新算法提出一种改进的参数选择方法以大大减少公钥参数数量,且能在标准模型下得到安全证明。

关键词 基于身份的数字签名,标准模型,短的公钥参数
中图法分类号 TN918.1 **文献标识码** A

Short Public Key Provable Security Identity-based Signature Scheme

WANG Zhi-yi[1] LIU Tie[2] KANG Li[1] XIE Jing[1] LEI Gang[1]
(School of Economics Information Engineering, Southwestern University of Finance & Economics, Chengdu 610074, China)[1]
(IBM Research-China, Beijing 100193, China)[2]

Abstract In the standard model an UCMA security IBS scheme was proposed by Paterson and Schuldt, which was based on computational Diffie-Hellman problem in bilinear pairing group. Two independent Waters' identity hash functions were directly employed to treat the user's identity and the signature message, respectively, so PS's IBS scheme had a great number of public keys. An improved parameters selecting method was proposed in the new scheme, which only needs a small number of public keys, and the new scheme can be proved security in the standard model.

Keywords Identity-based signature, Standard model, Short public key

1 引言

基于身份的密码系统(Identity-based Cryptosystem, IBC)[1]的一个重要应用是基于身份的数字签名方案(Identity-based Signature, IBS)。在基于身份的数字签名方案中,签名验证者在收到签名时不需先对签名验证公钥归属的真实性进行判断,如查询公钥证书、验证证书等,而直接使用约定的用户身份信息组合系统的主公钥对签名进行验证,这样将大大减小验证者的计算开销。

基于身份的密码系统IBC和数字签名方案有着紧密的联系,在IBC系统中可信任中心(Trusted Author, TA)向用户发放私钥的过程就是用TA的主私钥对用户身份信息进行认证,而认证可以看成是用TA主私钥对用户身份信息进行签名。Waters给出了从其IBE方案到普通签名方案的转化方法[2],对消息签名就是把消息视为身份并为该消息(身份)提供用户私钥,签名即是关于该消息的用户私钥;验证过程中用该消息(视为一次性身份)加密一随机数,如果能用用户私钥(签名)解密还原出随机数,那么签名正确,反之签名错误。

BMW方案中[3],BMW指出构造CCA安全的IBE方案,它可以用两套独立的Waters身份处理函数,一套用于真实身份处理,另一套用于处理密文消息。基于身份的数字签名方案设计同样可以利用这种消息处理方法。

2006年,Paterson和Schuldt(PS)利用Waters CPA IBE算法和BMW方案中提到的构造CCA安全IBE算法的思路,在标准模型下构造了双线性映射群下基于计算DH难题的UCMA安全的基于身份数字签名算法[4]。PS算法直接利用Waters方案中TA分发的用户私钥作为IBS中的用户私钥,并用另一套Waters身份处理函数处理消息,将用户私钥和Waters身份处理函数处理后的消息直接相乘来构成新的IBS签名。由于PS算法直接使用了两组独立的Waters身份处理函数,因此算法中公钥参数数量巨大。

2008年,Narayan和Parampalli在PS的IBS签名算法基础上给出了新的IBS算法[5],新算法附带有接收者认证特性,能确保接收到的签名来自指定的签名者。由于该算法仍然直接使用两组独立的Waters身份处理函数,算法公钥参数数量未能得到优化(减少)。

2009年,李-姜在PS的IBS签名算法基础上给出了新的IBS算法[6],新算法虽然减少了签名验证时的计算量,但需要

到稿日期:2010-04-30 返修日期:2010-08-10 本文受国家自然科学基金青年项目"电子商务协议交易相关安全属性的形式化验证"(60903201)资助。

王之怡(1964—),男,博士生,副教授,主要研究方向为信息安全、电子支付系统,E-mail:wangzy@swufe.edu.cn;刘 铁(1975—),男,博士,高级研究员,主要研究方向为模式识别、商务智能;康 立(1980—),男,博士,讲师,主要研究方向为信息安全、密码学;谢 静(1987—),女,硕士,主要研究方向为电子支付系统;雷 刚(1987—),男,硕士,主要研究方向为商务智能。

进行相应的预计算，这样进一步增加了其算法的公钥参数数量。

本文基于 PS IBS 签名算法提出一种改进的公钥参数选择方法，在只增加少许计算负担而不增加任何签名通信量的条件下将大大减少 IBS 签名算法中公钥参数的使用数量，新算法能形式化地在标准模型下被证明 UCMA 是安全的，安全性仍基于在双线性映射群下计算 DH 难题。

2 基于身份的数字签名算法定义和安全模型

基于身份签名算法由以下算法组成：

系统建立 Setup(k)：一个可信任的用户私钥分发中心(TA)输入安全参数 $k\in Z$，输出主公钥 MPK 和主私钥 MSK。

私钥提取 $Der_{MSK}(ID)$：根据输入主私钥 MPK 和身份 ID，选择随机数 r，输出关于身份的私钥 $d_{ID}=Der_{MSK}(ID,r)$。

签名 $S_{MPK}(d_{ID},M)$：输入主公钥 MPK、消息 M 和用户身份 ID 的私钥 d_{ID}，选择随机数 t，输出签名 $\sigma=S_{MPK}(d_{ID},M,t)$。

验证 $V_{ID}(M,\sigma)$：输入系统主公钥 MPK、签名 σ、身份 ID，算法输出 1 表示签名正确，输出 0 表示签名不合法。

基于身份签名方案的安全性定义为：适应性选择身份，适应性选择消息攻击下的不可伪造签名(UCMA)安全，具体定义如下。

Adaptive-ID UCMA 安全性：称一个基于身份签名算法是 Adaptive-ID UCMA 安全的，是指任何概率多项式时间攻击者在以下游戏中攻击成功的优势可以忽略：

(1)挑战者运行 Setup(k)获得随机产生的主公私钥对(MPK,MSK)，然后将主公钥 MPK 发送给攻击者；

(2)攻击者适应性地选取身份 ID 进行私钥提取询问，挑战者用 $d_{ID}=Der_{MSK}(ID)$进行应答；

(3)攻击者适应性地选取身份和消息(ID,M)进行签名询问，挑战者先生成身份对应的私钥 $d_{ID}=Der_{MSK}(ID)$，再生成签名；

(4)最后，攻击者输出(σ^*,M^*,ID^*)，要求攻击者未询问过身份 ID^* 的私钥且未询问过(M^*,ID^*)的签名，如果攻击者输出的签名能通过验证，那么攻击者攻击成功。

3 基于身份的数字签名算法

设 G 和 G_1 为阶为素数 p 的循环群，g 为 G 上的生成元，$e:G\times G\to G_1$ 为可有效计算的双线性映射。

系统建立 Setup(k)：系统主公钥建立算法 TA 随机选取群 G 的生成元 g 和 $a\in Z_p$，计算 $g_1=g^a$；接着在群 G 中随机选择 u，g_2 和 m；最后随机独立选择 4 个抗碰撞 hash 函数 $H_1:\{0,1\}^*\to Z_p$；$H_2:\{0,1\}^*\to Z_{k_1}$；$H_3:\{0,1\}^*\times G\to Z_p$；$H_4:\{0,1\}^*\times G\to Z_{k_2}$；其中 k_1，k_2 的大小稍后确定。

系统的主公钥和主私钥为：

主公钥：$(g,g_1,g_2,u,m,H_1,H_2,H_3,H_4)$；

主私钥：(g_2^a)。

私钥提取 $Der_{MSK}(ID)$：为生成身份 v 的私钥，TA 随机选择 $r\in Z_p$，计算私钥为：

$d_0=g_2^a(ug^{H_1(ID)}g_2^{H_2(ID)})^r$，$d_1=g^r$

签名 $S_{MPK}(d_{ID},M)$：任意身份 v 的拥有者希望对消息 M 签名，签名者先随机选择 $r'\in Z_p$，对获得的私钥进行重随机化

$$d_0'=d_0(ug^{H_1(ID)}g_2^{H_2(ID)})^{r'}=g_2^a(ug^{H_1(ID)}g_2^{H_2(ID)})^{r+r'}$$

$$d_1'=d_1g^{r'}=g^{r+r'}$$

紧接着，签名者计算 $H_3(M,d_1')$ 和 $H_4(M,d_1')$，随机选择 $t\in Z_p$，生成身份 ID 对消息 M 的签名：

$$\begin{aligned}\sigma_0&=d_0'(mg^{H_3(M,d_1')}g_2^{H_4(M,d_1')})^t\\&=g_2^a(ug^{H_1(ID)}g_2^{H_2(ID)})^r(mg^{H_3(M,d_1')}g_2^{H_4(M,d_1')})^t\end{aligned}$$

$$\sigma_1=d_1'=g^r$$

$$\sigma_2=g^t$$

验证 $V_{ID}(M,\sigma)$：令(M,σ_0,σ_1,σ_2)为收到的签名，验证者计算 $H_3(M,\sigma_1)$和 $H_4(M,\sigma_1)$验证签名：

$$\begin{aligned}e(\sigma_0,g)=&e(g_1,g_2)e((ug^{H_1(ID)}g_2^{H_2(ID)}),\sigma_1)\\&e((mg^{H_3(M,d_1')}g_2^{H_4(M,d_1')}),\sigma_2)\end{aligned}$$

正确性：对一个正确的签名，有：

$$\begin{aligned}e(\sigma_0,g)=&e(g_2^a(ug^{H_1(ID)}g_2^{H_2(ID)})^r(mg^{H_3(M,d_1')}\\&g_2^{H_4(M,d_1')})^t,g)\\=&e(g_2^a,g)e((ug^{H_1(ID)}g_2^{H_2(ID)})^r,g)\\&e((mg^{H_3(M,d_1')}g_2^{H_4(M,d_1')})^t,g)\\=&e(g_1,g_2)e((ug^{H_1(ID)}g_2^{H_2(ID)}),\sigma_1)\\&e((mg^{H_3(M,d_1')}g_2^{H_4(M,d_1')}),\sigma_2)\end{aligned}$$

4 标准模型下新的 IBS 算法安全性证明

定理 1 令 H_1,H_2,H_3,H_4 是抗碰撞 hash 函数，假设在双线性映射群中计算 Diffie-Hellman(CDH)数学难题成立，那么上述基于身份的数字签名算法是能抗适应性选择消息伪造签名攻击(UCMA)的。

证明：如果攻击者 A 执行 UCMA 攻击上述基于身份的签名算法的优势为 $\varepsilon_A=Adv_{IBS,A}^{UCMA}$，那么能构造上述基于身份签名算法的仿真者 B 在至多执行 $O((q_E+q_S)(\log p)^3)$ 数量的群运算后能以优势 $\varepsilon_B=Adv_B^{CDH}$ 攻破 CDH 数学难题：

$$\varepsilon_B\geqslant\varepsilon_A\frac{1}{e\cdot(q_E)^2}$$

其中，q_E 是基于身份签名算法中攻击者 A 进行用户私钥提问次数的上界；q_S 是基于身份签名算法中攻击者 A 进行签名提问次数的上界。

证明：证明中仿真者 B 将利用攻击者 A 的攻击行为解 CDH 数学难题，具体步骤如下。

系统建立 Setup(k)：令群 G 的阶为素数 p，存在一个高效的到 G_1 的双线性映射，表示为 $e:G\times G\to G_1$。首先仿真者 B 从 CDH 数学难题挑战处获得(g,g^a,g^b)；接着随机独立选择 4 个抗碰撞 hash 函数 $H_1:\{0,1\}^*\to Z_p$；$H_2:\{0,1\}^*\to Z_{k_1}$；$H_3:\{0,1\}^*\times G\to Z_p$；$H_4:\{0,1\}^*\times G\to Z_{k_2}$；其中 k_1，k_2 的大小稍后确定；然后，B 在 Z_p 中随机独立选择 x_1 和 x_2；在 Z_{k_1} 和 Z_{k_2} 中分别随机独立选择 y_1 和 y_2；令 $g_1=g^a$ 和 $g_2=g^b$ 并计算 $u=g^{x_1}g_2^{-y_1}$ 和 $m=g^{x_2}g_2^{-y_2}$。

B 公布系统主公钥，保留系统主私钥。

主公钥：$(g,g_1,g_2,u,m,H_1,H_2,H_3,H_4)$；

主私钥：(g_2^a(未知)，x_1，y_1，x_2 和 y_2)。

用户私钥询问：攻击者 A 进行用户私钥询问，他给出身份 ID，仿真者 B 首先测试 $H_2(ID)=y_1$，如果成立将终止仿真($Abort_q$)，反之随机选择 $r\in Z_p$ 并在未知主私钥 g_2^a 的条件下给出关于 ID 的用户私钥(d_0,d_1)：

$$d_0 = g_1^{\frac{H_1(ID)+x_1}{H_2(ID)-y_1}} (ug^{H_1(ID)} g_2^{H_2(ID)})^r$$
$$= g_2^a (g_2^{H_2(ID)-y_1} g^{H_1(ID)+x_1})^{-\frac{a}{H_2(ID)-y_1}} (ug^{H_1(ID)} g_2^{H_2(ID)})^r$$
$$= g_2^a (ug^{H_1(ID)} g_2^{H_2(ID)})^{-\frac{a}{H_2(ID)-y_1}} (ug^{H_1(ID)} g_2^{H_2(ID)})^r$$
$$= g_2^a (ug^{H_1(ID)} g_2^{H_2(ID)})^{\tilde{r}}$$
$$d_1 = g_1^{\frac{1}{H_2(ID)-y_1}} g^r = g^{\tilde{r}}$$

其中，$\tilde{r}=r+\frac{-a}{H_2(ID)-y_1}$（未知），可以看出这是关于身份 ID 的合法私钥。

签名询问：攻击者 A 进行签名询问给出(ID,M)，仿真者 B 首先测试 $H_2(ID)\neq y_1$，如果成立，B 将按照上述用户私钥生成算法计算出关于身份 ID 的私钥，利用正常签名过程给出签名；如果 $H_2(ID)=y_1$，仿真者 B 将随机选择 $r\in Z_p$，计算 $H_4(M,g^r)$并测试 $H_4(M,g^r)=y_2$，如果成立，重新选择 $r\in Z_p$ 直到满足 $H_4(M,g^r)\neq y_2$ 为止；然后随机选择 $t\in Z_p$ 并给出关于(ID,M)的签名$(\sigma_0,\sigma_1,\sigma_2)$：

$$\sigma_0 = (ug^{H_1(ID)} g_2^{H_2(ID)})^r g_1^{\frac{H_3(M,g^r)+x_2}{H_4(M,g^r)-y_2}} (mg^{H_3(M,g^r)} g_2^{H_4(M,g^r)})^t$$
$$= (ug^{H_1(ID)} g_2^{H_2(ID)})^r (mg^{H_3(M,g^r)} g_2^{H_4(M,g^r)})^t g_2^a (g^{H_3(M,g^r)+x_2} g_2^{H_4(M,g^r)-y_2})^{-\frac{a}{H_4(M,g^r)-y_2}}$$
$$= (ug^{H_1(ID)} g_2^{H_2(ID)})^r (mg^{H_3(M,g^r)} g_2^{H_4(M,g^r)})^t g_2^a (mg^{H_3(M,g^r)} g_2^{H_4(M,g^r)})^{-\frac{a}{H_4(M,g^r)-y_2}}$$
$$= g_2^a (ug^{H_1(ID)} g_2^{H_2(ID)})^r (mg^{H_3(M,g^r)} g_2^{H_4(M,g^r)})^{t-\frac{a}{H_4(M,g^r)-y_2}}$$
$$\sigma_1 = g^r$$
$$\sigma_2 = (g_1)^{-\frac{1}{H_4(M,g^r)-y_2}} g^t = g^{t-\frac{a}{H_4(M,g^r)-y_2}}$$

假设存在一个未知的 $t'=t+\frac{-a}{H_4(M,g^r)-y_2}$，可以看出上述签名是关于$(ID,M)$的合法签名。

新算法将 $d_1=g^r$ 引入到对签名消息的处理，实际签署的消息变为 $H_4(M,g^r)$，这样的变化可以确保仿真者能回答攻击者 A 提出的任何签名询问而不会终止仿真。

伪造签名输出：经过用户私钥询问和签名询问，攻击者将给出关于(ID^*,M^*)的伪造签名$(\sigma_0^*,\sigma_1^*,\sigma_2^*)$，要求身份 ID^* 未进行过私钥询问且(ID^*,M^*)未进行过签名询问，仿真者先对伪造签名进行验证，若不能通过验证将拒绝该伪造签名；反之仿真者将计算 $H_4(M^*,\sigma_1^*)$ 和 $H_2(ID^*)$并测试 $H_4(M^*,\sigma_1^*)=y_2$ 和 $H_2(ID^*)=y_1$，如果有一式不成立，仿真者将终止$(Abort_o)$，反之两式均成立，B 可计算输出 g^{ab}：

$$g^{ab} = \left(\frac{\sigma_0^*}{(\sigma_1^*)^{H_1(ID^*)+x_1}(\sigma_2^*)^{H_3(M^*,g^r)+x_2}}\right)$$
$$= \left(\frac{g_2^a (ug^{H_1(ID^*)} g_2^{H_2(ID^*)})^r (mg^{H_3(M^*,g^r)} g_2^{H_4(M^*,g^r)})^t}{(\sigma_1^*)^{H_1(ID^*)+x_1}(\sigma_2^*)^{H_3(M^*,g^r)+x_2}}\right)$$
$$= \left(\frac{g_2^a (g_2^{H_2(ID^*)-y_1} g^{H_1(ID^*)+x_1})^r (g_2^{H_4(M^*,g^r)-y_2} g^{H_3(M^*,g^r)+x_2})^t}{(\sigma_1^*)^{H_1(ID^*)+x_1}(\sigma_2^*)^{H_3(M^*,g^r)+x_2}}\right)$$
$$= \left(\frac{g_2^a (g^{H_1(ID^*)+x_1})^r (g^{H_3(M^*,g^r)+x_2})^t}{(\sigma_1^*)^{H_1(ID^*)+x_1}(\sigma_2^*)^{H_3(M^*,g^r)+x_2}}\right)$$

在上述仿真证明过程中，由于条件限制仿真者将在私钥询问阶段终止仿真（$Abort_q$）和在伪造签名输出后终止仿真（$Abort_o$）。

为分析仿真系统运行时的不终止概率，我们定义如下 3 个事件：

事件 1　E_1 表示在上述仿真过程中所有的用户私钥询问满足 $H_2(ID)\neq y_1$；

事件 2　E_2 表示攻击者输出的签名满足 $H_2(ID^*)=y_1$；

事件 3　E_3 表示攻击者输出的签名满足 $H_4(M^*,\sigma_1)=y_2$。

由于 H_2 与 H_4 是随机独立选择的，且 x_1 和 x_2，y_1 和 y_2 也是随机独立选择的，因此事件 E_3 与 E_2 和 E_1 是独立的。

由于 H_4 是抗碰撞的 hash 函数，它的输出将在 Z_k 中均匀分布，因此 $\Pr[H_4(M^*,\sigma_1)=y_2]=1/k_2$，那么有 $\Pr[E_3]=\frac{1}{k_2}$。

类似地，$\Pr[H_2(ID)=y_1]=1/k_1$，假设在上述仿真过程中攻击者 A 总计进行了 q_E 次用户私钥询问，那么

$$\Pr[E_1]=\Pr[(\bigwedge_{i=1}^{q_E} H_2(ID)\neq y_1)]=(1-\frac{1}{k_1})^{q_E}\Pr[E_2\mid E_1]$$
$$=\frac{1}{k_1}$$

综上所述，仿真中不终止的概率为：

$$\Pr[\overline{Abort_q}\wedge\overline{Abort_o}]=\Pr[E_1]\Pr[E_2\mid E_1]\Pr[E_3]$$
$$=\frac{1}{k_1}(1-\frac{1}{k_1})^{q_E}\frac{1}{k_2}$$

根据基于身份数字签名算法的安全要求 $q_E=2^{30}$，在 $k_1=1+q_E$ 时：

$$\frac{1}{k_1}(1-\frac{1}{k_1})^{q_E}=\frac{1}{q_E}(1-\frac{1}{1+q_E})^{1+q_E}\approx\frac{1}{e\cdot q_E}$$

类似地取 $k_2=q_E$，那么仿真中系统不终止的概率为：

$$\Pr[\overline{Abort_q}\wedge\overline{Abort_o}]=\frac{1}{k_1}(1-\frac{1}{k_1})^{q_E}\frac{1}{k_2}=\frac{1}{e\cdot(q_E)^2}$$

因此，如果攻击者 A 能以优势 ε_A 攻击上述基于身份的数字签名算法，那么仿真者 B 能以如下优势攻击 CDH 数学难题：

$$\varepsilon_B\geqslant\varepsilon_A\frac{1}{e\cdot(q_E)^2}$$

5　算法比较

表 1 给出新算法和 PS 算法、李-姜算法的性能对比，表 2 给出符号定义。

表 1　验证计算量和公钥参数对比

算法	验证计算量	公钥参数数量
PS 算法	3E	(5+2n)G
李-姜算法	2E+exp	(4+n)G+(1+n)Z_p+2G_1
新算法	3E	5G

表 2　符号定义

符号	定义
E	Pairing 运算计算量
exp	指数运算计算量
G	G 中元素
Z_p	Z_p 中元素
G_1	G_1 中元素

说明：n 为安全参数，在现有安全要求下 n 的大小为 160，因此新算法使用的公钥参数数量较表中其它两种算法有了很大的减少，这将节约大量的存储空间。

结束语　基于 Waters CPA IBE 方案和 PS UCMA IBS 算法构造了新的基于身份数字签名算法。新的 IBS 算法改进

了参数选择方法，大大减少了公钥参数的使用；另外在消息处理中引入部分用户身份私钥来增加对随机消息的控制，使得在证明中可以容易生成任意身份和消息(ID,M)对的签名。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology Proceedings of Crypto '84. Berlin: Springer-Verlag, 1985: 47-53

[2] Waters B. Efficient identity-based encryption without random oracles[C]// Advances in Cryptology Proceedings of EuroCrypto 2005. Berlin: Springer-Verlag, 2005: 114-127

[3] Boyen X, Mei Q, Waters B. Direct chosen ciphertext security from identity-based techniques[C]// ACM Conference on Computer and Communications Security. New York: ACM CCS, 2005: 320-329

[4] Paterson K, Schuldt J. Efficient identity-based signatures secure in the standard model[C]// Advances in Cryptology Proceedings of ACISP 2006. Berlin: Springer-Verlag, 2006: 207-222

[5] Narayan M S, Parampalli U. Efficient identity-based signatures in the standard model[J]. IET Inf. Secur., 2008, 2(4): 108-118

[6] 李继国，姜平进. 标准模型下可证安全的基于身份的高效签名方案[J]. 计算机学报，2009，32(11)：2130-2136

(上接第 126 页)

为了测试算法鲁棒性，对嵌入水印后的图像进行了各种攻击。图 5 显示了算法在不同强度的高斯噪声攻击下的误码率，图 6 显示了算法在不同品质系数 JPEG 压缩攻击下的误码率，表 2 显示的是算法在其他常见攻击下的误码率。

需要说明的是，对于嵌入的水印为二值伪随机数来说，上述图表中的数据仅反映了一次实验结果，其中的某个值并不具有实际意义。从图表中的实验数据可以看出，本文算法对各种常见攻击都能保证一定的鲁棒性，对常见攻击的误码率均低于传统亮度方法的误码率。另外，在抵抗高斯噪声方面，本文算法效果优于文献[13]，当方差为 3.5%时，本文算法提取出的水印误码率分别为 Lena 图像：0.3037，Baboon 图像：0.2412，Avion 图像：0.3291。而在相同的攻击参数下，文献[13]中的算法已经不能抵抗高斯噪声攻击；在抵抗 JPEG 压缩攻击中，本文算法的表现也优于文献[13]，经品质系数为 10 的 JPEG 压缩攻击后，本文算法提取出的水印的误码率分别为 Lena 图像：0.3496，Baboon 图像：0.2695，Avion 图像：0.2923，而文献[13]中的算法在品质系数为 25 的 JPEG 压缩攻击下提取出的有意义的水印已经产生较大的失真。

表 2 算法鲁棒性测试数据(误码率)

攻击种类及参数		低通滤波(方差=1)			中值滤波			均值滤波	椒盐噪声	中央剪切
		3×3	5×5	7×7	3×3	5×5	7×7	3×3	0.02	1/16
Lena	单通道亮度法	0.0322	0.0352	0.0361	0.0020	0.0645	0.2158	0.0313	0.2031	0.0791
	本文四元数幅值调制法	0.0244	0.0322	0.0352	0.0010	0.0625	0.2119	0.0303	0.0342	0.0791
Baboon	单通道亮度法	0.0527	0.0898	0.0938	0.2559	0.4092	0.4277	0.0830	0.1113	0.0039
	本文四元数幅值调制法	0.0518	0.0889	0.0908	0.0262	0.2035	0.3344	0.0771	0.0195	0.0039
Avion	单通道亮度法	0.0859	0.1490	0.1577	0.0381	0.2100	0.3408	0.1080	0.0986	0.0654
	本文四元数幅值调制法	0.0869	0.1494	0.1582	0.0254	0.1783	0.3057	0.1094	0.0863	0.0654

结束语 将四元数模型在彩色图像处理中的应用进一步扩展到彩色图像数字水印领域，提出一种基于彩色图像四元数频域幅值调制水印算法。在对载体图像进行处理的过程中始终将彩色像素作为一个整体来处理，使得彩色通道间的光谱联系贯穿在对这个整体进行傅立叶变换以及幅值水印嵌入的过程中，在具有良好的不易感知性的同时，也保证了较好的抗攻击能力。基于四元数理论的彩色图像处理技术的研究尚处于起步阶段，理论体系还有待于进一步完善。本文的工作对四元数在彩色图像处理中的应用是很好的补充，为彩色图像的版权保护提供了一种新方法。

参 考 文 献

[1] Kutter M, Jordan F, Bossen F. Digital signature of color images using amplitude modulation[A]// SPIE[C]. 1997, 3022: 518-526

[2] 王向阳，杨红颖，候丽敏. 一种新的半脆弱彩色图像数字水印算法[J]. 自动化学报，2007，33(6)：561-566

[3] 李晓强，薛向阳. 基于多通道的彩色图像水印方案[J]. 计算机学报，2004，27(9)：1238-1244

[4] Pei S-C, Cheng C-M. Novel block truncation coding of color images using a quaternion- moment-preserving principle[J]. IEEE Transaction on Communication, 1997, 45(5): 583-595

[5] Cai C, Mitra S K. A normalized color difference edge detector based on quaternion representation[C]// Proceedings of the IEEE International Conference on Image Processing (ICIP). Vancouver, BC, Canada, 2000: 816-819

[6] Sangwine S J, Evans C J, Ell T A. A colour-sensitive edge detection using hypercomplex filtersz[C]// Proceedings of the 10th European Signal Processing Conference (EUSIPCO). Tampere, Finland, 2000, 1: 107-110

[7] Sangwine S J, Ell T A. Hypercomplex auto- and cross-correlation of color image[C]// Proceedings of the IEEE International Conference on Image Processing (ICIP). Kobe, Japan, 1999: 319-322

[8] Sangwine S J, Ell T A. Colour image filters based on hypercomplex convolution[J]. IEEE Proceedings-Vision, Image and signal Processing, 2000, 147(2): 89-93

[9] Sangwine S J, Ell T A. Hypercomplex Fourier Transforms of Color Images [J]. IEEE Transactions on Image Processing, 2007, 16(1): 22-35

[10] Sangwine S J, Ell T A. Hypercomplex operators and vector correlation[C]// Proc. EUSIPCO XI European Signal Processing Conf. Toulouse, France, Sep. 2002, III: 247-250

[11] Bas P, Bihan N L, Chassery J-M. Color image watermarking using quaternion Fourier transform [C]// IEEE International Conference on Acoustics, Speech, and Signal Processing. 2003: 521-524

[12] Ell T A, Sangwine S J. Decomposition of 2D Hyper- complex Fourier Transforms into Pairs of Complex Fourier Transforms [C]// European Signal Processing Conference (EUSIPCO). Tampere, Finland, 2000: 151-154

[13] 江淑红，张建秋，胡波. 一种超复数频域的有意义数字水印算法[J]. 系统工程与电子技术，2009，31(9)：2242-2248