



(12) 发明专利

(10) 授权公告号 CN 101895539 B

(45) 授权公告日 2013.03.20

(21) 申请号 201010223892.3

CN 101488856 A, 2009.07.22,

(22) 申请日 2010.07.07

审查员 李晓玲

(73) 专利权人 武汉大学

地址 430072 湖北省武汉市武昌珞珈山

(72) 发明人 徐正全 蒋力 徐彦彦

(74) 专利代理机构 武汉科皓知识产权代理事务所 (特殊普通合伙) 42222

代理人 张火春

(51) Int. Cl.

H04L 29/06 (2006.01)

(56) 对比文件

DE 60321009 D1, 2008.06.26,

CN 1343420 A, 2002.04.03,

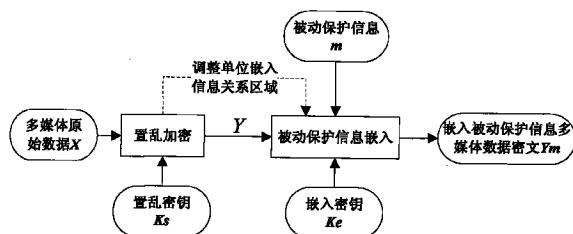
权利要求书 1 页 说明书 6 页 附图 3 页

(54) 发明名称

基于置乱的多媒体数据主动加密与被动保护结合的方法

(57) 摘要

本发明涉及多媒体数据安全保护技术领域，尤其涉及一种基于置乱的多媒体数据主动加密与被动保护结合的方法。本发明一方面对多媒体数据提供主动加密保护，在网络传输、存储等过程中保护数据内容免受侵害的同时，可在密文中方便嵌入、提取被动保护信息，利于实现第三方验证；另一方面在多媒体数据解密后又能为其提供被动保护，明确多媒体数据版权信息，且在数据泄露后能对泄密者进行追踪，锁定传播途径。本发明基于置乱主动加密，实现了多媒体数据主动加密与被动保护的有效结合，无需解密，可在多媒体数据密文中直接嵌入、提取被动保护信息，在多媒体数据解密后，被动保护信息仍然留存于多媒体数据明文中。



1. 一种多媒体数据的主动置乱加密和被动保护信息嵌入的方法,其特征在于,包括以下步骤:

①根据加密密钥 K_s 对原始多媒体数据 X 进行置乱加密,获取多媒体数据密文 Y ,置乱单位为单位数据或多单位数据区域;

②根据上述步骤所采用的置乱单位,调整被动保护信息嵌入算法,使得被动保护单位信息的嵌入关系域包含于置乱单位中;

③根据嵌入密钥 K_e ,将原始的被动保护信息明文 m 嵌入至多媒体数据密文 Y ,获取嵌入被动保护信息密文 Y_m 。

2. 根据权利要求 1 所述的多媒体数据的主动置乱加密和被动保护信息嵌入的方法,其特征在于:

步骤①中所述单位数据为位或者像素;

步骤①中多媒体数据置乱加密过程可通过 Arnold 变换或其他置乱方法实现;

步骤③中被动保护信息嵌入过程可通过抖动调制或其他嵌入方法实现。

3. 根据权利要求 1 所述的多媒体数据的主动置乱加密和被动保护信息嵌入的方法,其特征在于:从嵌入被动保护信息密文 Y_m 直接提取被动保护信息明文 m ,包括以下步骤:

①根据加密密钥 K_s ,由置乱单位确定被动保护单位信息的嵌入区域;

②根据嵌入密钥 K_e ,从嵌入被动保护信息密文 Y_m 中提取原始的被动保护信息明文 m 。

4. 一种多媒体数据的主动置乱解密和被动保护信息提取的方法,其特征在于,包括以下步骤:

①根据加密密钥 K_s ,对嵌入被动保护信息密文 Y_m 进行置乱解密操作,获取嵌入了被动保护信息密文 w 的嵌入被动保护信息明文 X_w ;

②根据嵌入密钥 K_e ,从嵌入被动保护信息明文 X_w 中提取被动保护信息密文 w ;

③根据加密密钥 K_s ,求取解密操作逆置乱的逆操作,此时的置乱单位为嵌入载体置乱单位区域中的所有被动保护信息密文 w ;

④按照步骤③得到的逆操作,对从嵌入被动保护信息明文 X_w 中提取的被动保护信息密文 w 进行解密,获取原始的被动保护信息明文 m 。

基于置乱的多媒体数据主动加密与被动保护结合的方法

技术领域

[0001] 本发明涉及多媒体数据安全保护技术领域,尤其涉及一种基于置乱的多媒体数据主动加密与被动保护结合的方法。

背景技术

[0002] 进入二十一世纪以来,数字技术的发展及 Internet 的普及给图像、视频、语音等各种媒体数据的存储、传播及发布带来了极大的便利。但与此同时,多媒体数据的安全问题日益突出。现今用于多媒体数据安全保护的方法大体可分为:主动保护和被动保护。所谓主动保护,就是防止被保护数据免于非授权用户侵害的安全保护方法,加密是主动保护最主要的实现手段。而被动保护,则是在数据安全受到侵害后,提供完整性鉴定、身份证明等属性信息,用于追踪不法者的安全保护手段。数字水印及数字指纹是最主要的两种被动保护手段。为此,可通过主动加密手段,保证多媒体数据在传输、存储等过程中避免非授权用户的侵害。但在授权用户解密后,主动加密的保护性就不复存在。无法防止授权用户非法泄露解密后的数据,更不能对泄密者进行追踪。且在版权利益极大的当今社会,数据所有者并不能证明其对解密后数据的所有权,对此,不法者可通过盗版牟取暴利,极大损害数据所有者的利益。因此,仅依靠主动加密无法对多媒体数据提供完全有效的保护,还迫切需要被动的安全保护机制。在多媒体数据安全受到侵害后,明确数据版权,追究不法者责任,为多媒体数据的使用给予监督和控制,提供更深层次的保护。

[0003] 然而,现阶段,若想对多媒体数据进行主动保护的同时提供被动保护,只能将两者进行简单的叠加。叠加方式有两种:在原始数据中加入数字水印或数字指纹进行被动保护后再进行主动加密;在主动加密之后再在密文中添加被动保护措施。然而这两种方式都存在着很大的弊端。对于第一种方式,由于被动保护信息存在于原始数据中,则每次进行被动保护验证时,都必须首先进行解密操作。更值得注意的是,在提取被动保护信息过程中,多媒体数据必须以明文的形式存在,不利于引入第三方验证,且对其安全更是一个很大的威胁。第二种方式,虽然避免了第一种方式的缺陷但其不足之处也是显而易见,被动保护信息嵌入后带来的数据改变会影响解密,有可能造成关键数据不可恢复。为了避免此种情况,解密前不得不再次对被动保护信息进行修改,而此时,多媒体数据解密后被动保护将不复存在。

[0004] 一方面,多媒体数据要求主动保护的同时受到被动保护;另一方面,主动、被动保护并不能实现契合。由此,多媒体数据的主动被动安全保护相结合的问题亟待解决。

发明内容

[0005] 针对上述存在的技术问题,本发明的目的是提供一种基于置乱的多媒体数据主动加密与被动保护结合的方法,以实现多媒体数据主动加密和被动保护相结合。

[0006] 为达到上述目的,本发明采用如下的技术方案:

[0007] 一种多媒体数据的主动置乱加密和被动保护信息嵌入的方法,包括:

[0008] ①根据加密密钥 K_s 对原始多媒体数据 X 进行置乱加密, 获取多媒体数据密文 Y , 置乱单位为单位数据或多单位数据区域;

[0009] ②根据上述步骤所采用的置乱单位, 调整被动保护信息嵌入算法, 使得被动保护单位信息的嵌入关系域包含于置乱单位中;

[0010] ③根据嵌入密钥 K_e , 将原始被动保护信息 m 嵌入至多媒体数据载体密文 Y , 获取嵌入被动保护信息载体密文 Y_m 。

[0011] 步骤①中所述单位数据为位或者像素;

[0012] 步骤①中多媒体数据置乱加密过程可通过 Arnold 变换或其他置乱方法实现;

[0013] 步骤③中被动保护信息嵌入过程可通过抖动调制或其他嵌入方法实现。

[0014] 一种基于多媒体数据密文的被动保护信息提取方法, 其特征在于, 包括以下步骤:

[0015] ①根据加密密钥 K_s , 确定被动保护单位信息的嵌入区域;

[0016] ②根据嵌入密钥 K_e , 从多媒体数据密文 Y_m 中提取被动保护嵌入信息 m ;

[0017] 一种多媒体数据的主动置乱解密和被动保护信息提取的方法, 包括:

[0018] ①根据加密密钥 K_s , 对嵌入被动保护信息的多媒体数据密文 Y_m 进行置乱解密操作, 获取嵌入被动保护信息的多媒体数据明文 X_w ;

[0019] ②根据嵌入密钥 K_e , 从解密后的多媒体数据明文 X_w 中提取被动保护嵌入信息 w ;

[0020] ③根据加密密钥 K_s , 求取多媒体数据密文解密逆置乱操作的逆操作, 此时的置乱单位为嵌入载体置乱单位区域中的所有被动保护信息;

[0021] ④按照步骤③得到的逆操作, 对从解密后的多媒体数据明文 X_w 中提取被动保护嵌入信息 w 进行解密, 获取被动保护嵌入信息明文 m 。

[0022] 一种基于置乱的多媒体数据主动加密与被动保护结合方法, 包括:

[0023] 对多媒体数据进行置乱加密获取多媒体数据密文, 根据采用的置乱单位确定被动保护信息嵌入区域后, 将被动保护信息嵌入多媒体数据载体获取嵌入被动保护信息的多媒体数据密文;

[0024] 从嵌入了被动保护信息的多媒体数据密文中根据提取算法直接提取被动保护信息明文, 在多媒体数据密文进行逆置乱恢复多媒体数据明文后, 根据提取算法, 获得多媒体载体明文中提取出被动保护嵌入信息, 通过相应的逆置乱操作恢复被动保护嵌入信息明文。

[0025] 本发明具有以下优点和积极效果:

[0026] 1) 基于置乱主动加密, 实现了多媒体数据主动加密与被动保护的有效结合, 无需解密, 可在多媒体数据密文中直接嵌入、提取被动保护信息, 在多媒体数据解密后, 被动保护信息仍然留存于多媒体数据明文中;

[0027] 2) 对置乱主动加密及被动保护信息的嵌入方法并没有特殊规定, 具有一定的普遍性。

附图说明

[0028] 图 1 是本发明的多媒体数据加密和被动保护信息嵌入过程框图。

[0029] 图 2 是本发明的多媒体数据被动保护信息提取和解密过程框图。

[0030] 图 3 是本发明基于 Arnold 置乱及 DCT 域抖动调制对图像数据进行加密和水印嵌入的系统框图。

[0031] 图 4 是本发明实施例提供的原始图像及被动保护嵌入信息。

[0032] 图 5 是本发明实施例中嵌入被动保护信息的图像密文及其提取的被动保护信息。

[0033] 图 6 是本发明实施例中嵌入被动保护信息的图像明文及其提取的被动保护信息。

具体实施方式

[0034] 本发明的目的在于实现多媒体数据主动加密和被动保护相结合,一方面对多媒体数据提供主动加密保护,在网络传输、存储等过程中保护数据内容免受侵害的同时,可在密文中方便嵌入、提取被动保护信息,利于实现第三方验证;另一方面在多媒体数据解密后又能为其提供被动保护,明确多媒体数据版权信息,且在数据泄露后能对泄密者进行追踪,锁定传播途径。

[0035] 由于选取的主动加密为空间置乱,其通过打乱多媒体数据空间排列实施主动加密保护,对于数字水印、数字指纹等通过修改载体数据嵌入保护信息的被动保护不会产生本质上的干扰。因此,本发明能够实现从多媒体数据密文中,无需解密,直接嵌入、提取被动保护嵌入信息;且经逆置乱解密后,被动保护信息仍然留存于多媒体数据明文中。

[0036] 主动保护,就是防止被保护数据免于非授权用户侵害的安全保护方法,加密是主动保护最主要的实现手段。而被动保护,则是在数据安全受到侵害后,提供完整性鉴定、身份证明等属性信息,用于追踪不法者的安全保护手段。数字水印及数字指纹是最主要的两种被动保护手段。

[0037] 基于周期置乱的多媒体数据主动加密与被动保护结合方法,包括步骤如下:

[0038] 第一步,多媒体数据的主动置乱加密和被动保护信息嵌入。对多媒体数据进行置乱加密获取多媒体数据密文,根据采用的置乱单位确定被动保护信息嵌入区域后,将被动保护信息嵌入多媒体数据载体获取嵌入被动保护信息的多媒体数据密文。

[0039] 第二步,多媒体数据的主动置乱解密和被动保护信息提取。从嵌入了被动保护信息的多媒体数据密文中可根据提取算法直接提取被动保护信息明文。在多媒体数据密文进行逆置乱恢复多媒体数据明文后,根据提取算法,仍然可从多媒体载体明文中提取出被动保护嵌入信息,但此时提取出的被动保护信息为其原文经载体逆置乱操作后的置乱密文,需通过相应的逆置乱操作恢复被动保护嵌入信息明文。

[0040] 本发明实现多媒体数据主动加密与被动保护结合方法中,对多媒体数据的主动置乱加密和被动保护信息嵌入的步骤如下:

[0041] 第一步,根据加密密钥 Ks(置乱操作参数)对原始多媒体数据 X 进行置乱加密,获取多媒体数据密文 Y,其中置乱操作可为 Arnold 置乱或其他置乱,置乱单位可为单位数据也可为多单位数据区域。

[0042] Arnold 置乱是公知的置乱算法,在此不予详细描述。

[0043] Arnold 变换,俗称猫脸变换,是 V. J. Arnold 提出的一种混沌映射,其具有典型的产生混沌运动的特性:拉伸和折叠,此外其还具有可逆性及周期性。Arnold 置乱公式在实例中给出。

[0044] 第二步,根据第一步所采用的置乱单位,调整被动保护信息嵌入算法,使得被动保

护单位信息的嵌入关系域包含于置乱单位中。

[0045] 第三步,根据嵌入密钥 Ke(被动保护信息嵌入操作参数),将原始被动保护信息 m 嵌入至多媒体数据载体密文 Y,获取嵌入被动保护信息载体 Ym,被动保护信息嵌入过程可通过抖动调制或其他嵌入方法实现。

[0046] 本发明实现多媒体数据主动加密与被动保护结合方法中,从嵌入了被动保护信息的多媒体数据密文中能够直接提取出被动保护信息明文 m。此时,只需根据嵌入密钥 Ke(被动保护信息嵌入操作参数)即可从多媒体数据密文中直接提取出被动保护信息原文。

[0047] 本发明实现多媒体数据主动加密与被动保护结合方法中,对多媒体数据进行逆置乱解密和从多媒体数据明文中提取被动保护信息的步骤如下:

[0048] 第一步,根据加密密钥 Ks,对嵌入被动保护信息的多媒体数据密文 Ym 进行置乱解密操作,获取嵌入被动保护信息的多媒体数据明文 Xw。

[0049] 第二步,根据嵌入密钥 Ke,从解密后的多媒体数据明文 Xw 中提取被动保护嵌入信息 w。

[0050] 第三步,根据加密密钥 Ks,求取多媒体数据密文解密逆置乱操作的逆操作,此时的置乱单位为嵌入载体置乱单位区域中的所有被动保护信息。

[0051] 若采用 Arnold 变换等具有周期性的置乱加密,在进行了 N1 次置乱操作后的多媒体数据密文中嵌入被动保护信息原文,当嵌入了被动保护信息的多媒体数据密文经 N2(N1+N2 = nN,其中 n 为整数,N 为所选取置乱操作的周期)次置乱恢复明文时,被动保护嵌入信息以密文形式存在于多媒体数据中。此时提取的被动保护信息密文,为其原文经 N2 次置乱结果,根据该置乱操作的周期性,只需对其进行 $N1' = N - (N2 \bmod N)$ 次置乱操作即可恢复明文。

[0052] 若采用其他未具备周期性的置乱操作,则要求其置乱及逆置乱互为逆操作,即置乱后可通过逆置乱恢复,而先进行逆置乱再经置乱操作也可恢复原始数据。此时,从经过逆置乱解密的载体明文中提取的被动保护嵌入信息密文通过相应的逆操作即可获取被动保护嵌入信息明文。

[0053] 第四步,按照第三步得到的逆操作,对从解密后的多媒体数据明文 Xw 中提取被动保护嵌入信息 w 进行解密,获取被动保护嵌入信息明文 m。

[0054] 下面结合附图对本发明的技术方案进行详细描述:

[0055] 如图 1 所示,本发明提供的实现多媒体主动加密与被动保护结合方法的具体步骤如下:

[0056] 1.1 原始多媒体数据加密。根据加密密钥 Ks 对原始多媒体数据进行置乱加密,置乱单位可为单位数据也可为多单位数据组成区域。其中单位数据可为 bit、像素等。

[0057] 1.2 被动保护嵌入单位信息关系区域选取。根据 1.1 中所选取的置乱单位调整被动保护单位嵌入信息关系区域,使得单位被动保护嵌入信息关系区域仅包含于某一置乱单位中,而一置乱单位可嵌入多个被动保护单位嵌入信息。

[0058] 1.3 被动保护信息嵌入操作。根据嵌入密钥 Ke,在 1.2 选取的被动保护嵌入单位信息关系区域范围内嵌入原始被动保护信息,得到嵌入了被动保护信息的多媒体数据密文 Ym。

[0059] 2. 根据上述多媒体数据加密步骤,其解密时,在加密密钥 Ks 的控制下,对多媒体

数据密文 Y_m 进行逆置乱操作得到多媒体数据明文 X_w 。此时, 置乱单位与加密过程中必须保持一致。

[0060] 3. 结合图 2, 本发明多媒体被动保护信息提取可同时在多媒体载体密文及明文下实现:

[0061] 3.1 多媒体密文提取被动保护信息。由于被动保护信息是以明文的形式嵌入至多媒体数据密文中, 因此从多媒体数据密文中, 根据嵌入密钥 K_e 即可直接提取出被动保护信息明文 m , 其提取过程为嵌入过程的逆操作。

[0062] 3.2 多媒体明文提取被动保护信息。由于被动保护信息是以明文的形式嵌入多媒体数据密文中, 在多媒体数据密文经逆置乱解密后, 相当于对嵌入其中的被动保护信息明文进行了置乱操作。此时被动保护信息将以密文 w 的形式存在于多媒体数据明文中。则从多媒体数据明文提取被动保护信息明文 m 的步骤如下:

[0063] 3.2.1 根据嵌入密钥 K_e , 从多媒体数据明文中提取嵌入被动保护信息 w , 此时, 提取的被动保护信息为置乱密文。

[0064] 3.2.2 根据置乱密钥 K_s , 确定对多媒体数据密文进行解密时所采取的逆置乱操作的逆操作。

[0065] 3.2.3 根据 3.2.2 提供的逆操作, 对提取的被动保护信息密文 w 进行解密, 获取被动保护信息明文 m 。

[0066] 4. 以图像数据为例, 基于 Arnold 变换及 8×8 分块 DCT 抖动调制, 本发明实现图像数据主动加密与被动保护结合方法的过程框图如图 3 所示。设被保护载体为 $N \times N$ 的灰度图像 X (若载体为彩色图像则选取其亮度分量进行处理), 嵌入的被动保护信息为 $n \times n$ 的二值图像 m 。考虑到 8×8 分块 DCT, 则取 $n = N/8$, 此时, 每个 8×8 DCT 变换块中只嵌入 1bit 被动保护信息, 即在图像载体主动置乱加密时以 8×8 区域为置乱单位, 在被动保护信息密文解密时以 1bit 为置乱单位。在被动保护信息嵌入时, 考虑到被动保护信息的不可见性以及鲁棒性, 选择在 8×8 DCT 系数块中的中频嵌入被动保护信息。则对图像实施基于 Arnold 周期置乱的主动加密与被动保护结合方法具体步骤如下:

[0067] 4.1 根据密钥 K_s , 对原始图像 X , 以 8×8 宏块为置乱单位, 进行 N_1 次 Arnold 置乱, 得到置乱图像 Y 。这里选取的 Arnold 置乱为广义 Arnold 置乱, 即其变换如下式所示:

$$[0068] \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \left[\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \right] (\bmod N) = \left[C \begin{pmatrix} x_i \\ y_i \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \right] (\bmod N)$$

[0069] 此时密钥 K_s 即为该 Arnold 置乱变换矩阵 C 及初始偏移量 (x_0, y_0) 。

[0070] 4.2 将载体置乱图像 Y 进行 8×8 分块 DCT。

[0071] 4.3 根据密钥 K_e , 在载体图像 DCT 变换宏块中频区域选取奇数个嵌入位, 按照 DCT 系数双极性量化法重复嵌入对应的被动保护信息 m_i 。设被动保护信息位 $m_i \in \{1, -1\}$, 选定的奇数 M 个嵌入位系数量化结果 Y_u^m 表示为:

[0072] 1) 若 $Y_u \in (2l\Delta, (2l+1)\Delta)$, 则

$$[0073] Y_u^m = \begin{cases} (2l+1)\Delta & m_i = 1 \\ 2l\Delta & m_i = -1 \end{cases}$$

[0074] 2) 若 $Y_u \in ((2l-1)\Delta, 2l\Delta)$, 则

$$[0075] \quad Y_u^m = \begin{cases} (2l-1)\Delta & m_i = 1 \\ 2l\Delta & m_i = -1 \end{cases}$$

[0076] 式中,下标 $0 < u < M$ 为 M 个 DCT 系数的序号。嵌入量化步长 Δ 由所选取的压缩量化步长决定。待被动保护信息全部嵌入后即得到嵌入了被动保护信息的载体密文 Y_m 。提取时,只需判断 M 个嵌入位 Y_u^w 的奇偶性即可提取被动保护信息:若 Y_u^m 中,奇数系数所占个数较多则嵌入的被动保护信息 $m_i = 1$,反之 $m_i = -1$ 。

[0077] 4.4 此时,嵌入了被动保护信息的主动置乱加密密文 Y_m 在未经解密的情况下,只需根据嵌入密钥 K_e 即可从载体密文中直接提取被动保护嵌入信息 m ,从而避免了载体信息的泄露,利于引入第三方验证。

[0078] 4.5 根据密钥 K_s ,利用 Arnold 置乱的周期性,对嵌入了被动保护信息的载体密文 Y_m 进行 N_2 次 8×8 宏块 Arnold 置乱,即可得到嵌入了被动保护信息的主动加密明文 X_w 。其中 $N_1+N_2 = a \cdot C(n)$, a 为非零整数, $C(n)$ 为 n 阶图像矩阵 Arnold 变换周期, n 为被动保护嵌入信息矩阵阶数。此时,被动保护信息以密文 w 的形式存在于载体明文 X_w 中,仅密钥 K_s 所有者才能提取被动保护信息,进一步提高了被动保护信息的安全性。

[0079] 4.6 根据嵌入密钥 K_e ,从载体明文中提取出被动保护信息密文 w 。

[0080] 4.7 被动保护信息密文解密。由于载体图像逆置乱解密的置乱单位为 8×8 宏块,且每宏块中仅嵌入 1bit 的被动保护信息,则提取的被动保护信息密文为其原文经 N_2 次 Arnold 变换所得。根据 Arnold 置乱的周期性,对 w 只需进行 $N_1' = N - (N_2 \bmod N)$ 次置乱操作即可恢复明文 m 。

[0081] 图 4 至图 6 给出了一幅 200×200 图像的实验结果。其中图 4a 为 200×200 原始载体图像,图 4b 为 25×25 原始被动保护信息二值图像;图 5a 为图 4a 嵌入了被动保护信息的置乱密文,图 5b 为从图 5a 中提取的被动保护信息;图 6a 为图 5a 解密后明文,图 6b 为从图 6a 中直接提取的被动保护信息密文,图 6c 为图 6b 经置乱解密后的提取被动保护信息明文。可见,本发明基于置乱,实现了多媒体数据的主动加密与被动保护相结合,在多媒体载体数据未解密的情况下能够直接嵌入、提取被动保护信息,且在多媒体数据解密后,被动保护信息仍然留存于载体明文中。

[0082] 上述实例用来解释说明本发明,而不是对本发明进行限制,在本发明的精神和权利要求的保护范围内,对本发明做出任何的修改和改变,都落入本发明的保护范围。

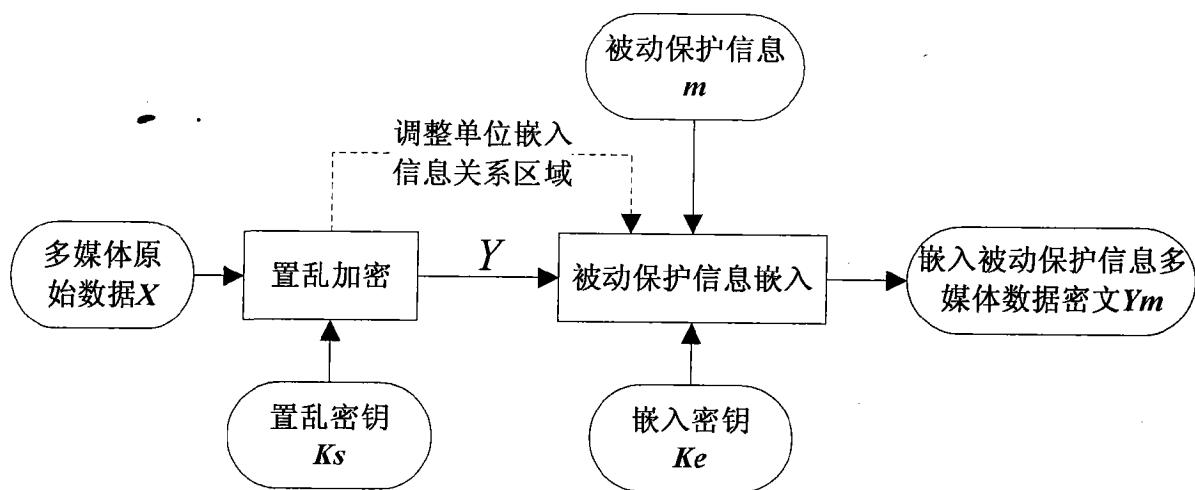


图 1

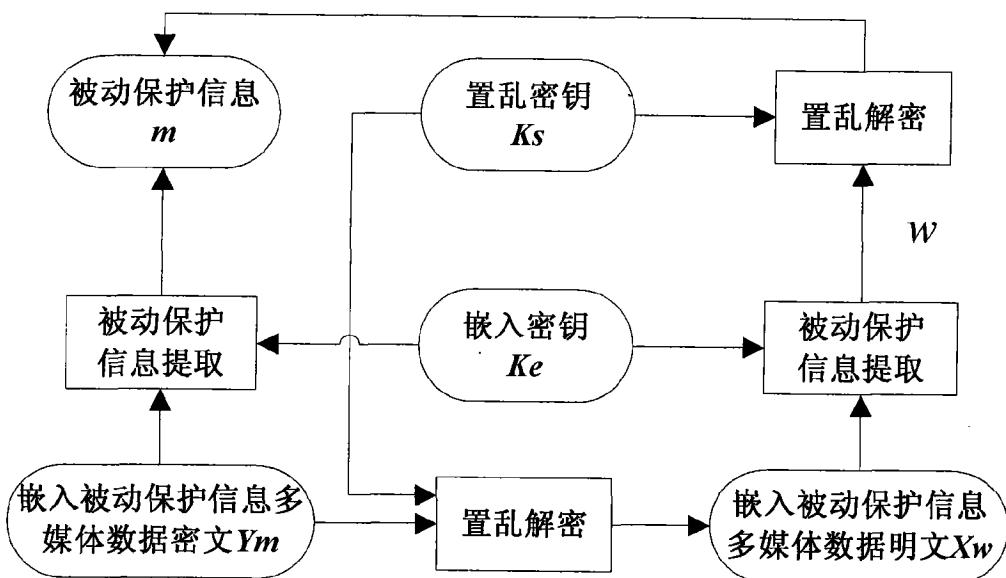


图 2

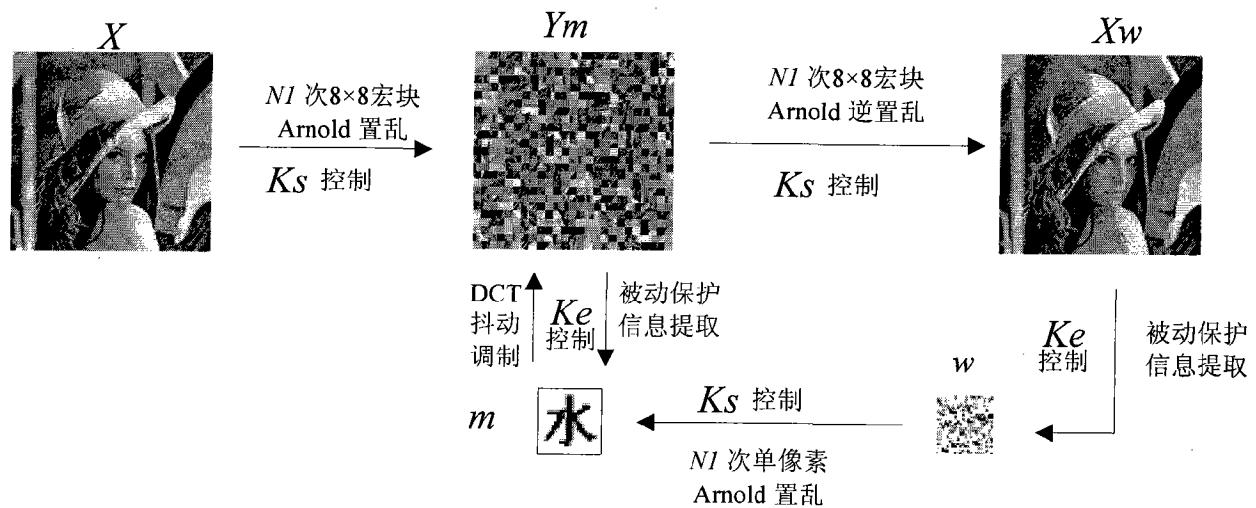
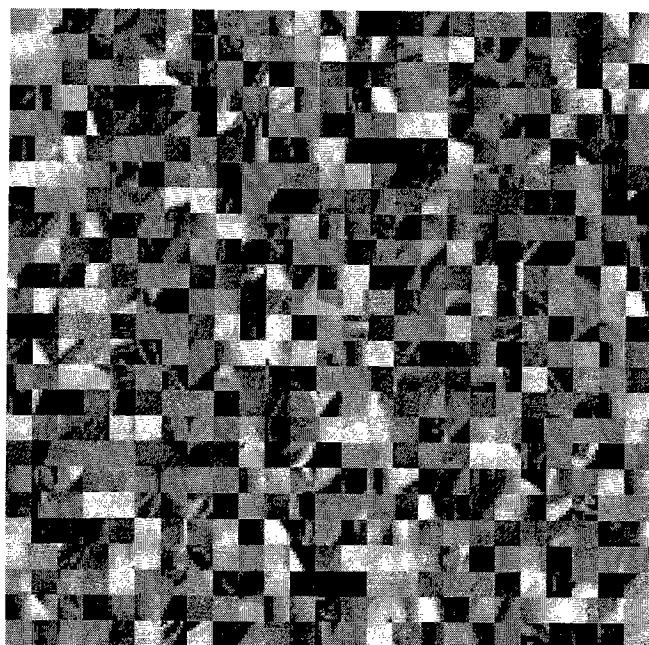


图 3



图 4



水

A

B

图 5



水

A

B

C

图 6