數位典藏環境之資料安全保護機制*

曹偉駿
大葉大學
資訊管理系
wjtsaur@mail.dyu.edu.tw

林宜進
大葉大學
資訊管理系
kimobbb@yahoo.com.tw

劉經緯
大葉大學
資訊管理系
gin_we@yahoo.com.tw

曾逸鴻
大葉大學
資訊管理系
aven@mail.dyu.edu.tw

摘要[1]

史料影像中加入典藏單位的數位浮水印，此技術只能保護單一的圖檔的防竄改。然而，數位典藏機構的檔案全文之詮釋由 Encoded Archival Description (EAD)文件與圖檔共同組合而成，若有心人士將某圖檔抽換成相同典藏單位但屬於不同文件的其他圖檔，則單純的數位浮水印將無法偵測出這樣的抽換影像攻擊。另外，EAD 文件與相對應之圖檔透過網路交換亦需提供安全性的保護機制，以防止有心人士將非法 EAD 文件或圖檔內容交換給其他典藏機構。是故，本研究將設計適用於數位典藏之安全的 EAD 資料保護機制。

關鍵字：
數位典藏、EAD、數位浮水印、資料保護

1. 前言

典藏資料為國家重要資產，數位典藏機構為了能讓典藏資料互相交換，以 Extensible Markup Language (XML)制定 Encoded Archival Description (EAD)為資料交換標準格式[15]，又將眾多典藏文物製作成數位圖片。其內容不只具有藝術價值，更有法律文獻公文資料，為歷史考查的依據。如果其數位內容遭受竄改或偽造不實的內容，不只館藏機構名譽受損，更會讓國家受到不白之冤。

數位典藏資數量龐大的史料文件與影像，包含了大量的知識與法律敘述，很希望讓大眾可以上網瀏覽觀看，但是又深怕有心人士竄改重要史料文件與影像之內容，並在外散播。因此，數位典藏機構亟需要考量典藏史料文件影像特性、與日後上網流通之電子檔案和 EAD 檔案，擬定並開發一套資料防竄改與資料保護之安全機制，並將此機制應用於典藏資料的交換。

數位典藏資料以以 XML 制定 EAD 資料交換方式，又將眾多典藏文物製作成數位圖片。實務上，要一項典藏文物記錄包括一份 EAD 檔案及數張數位圖片組成，其中 EAD 檔案記載該典藏資料的相關資訊，另外數位圖片則是該文物的不同角度或不同尺寸的實體照片。為了讓有心人士無法偽造出典藏機關所製作的數位史料，本論文將提出開發一套資料防竄改與資料保護之安全機制，以滿足現行典藏機構之安全需求。

由於 EAD 為 XML 資料格式，現行保護 XML 資料主要可利用 XML 數位簽章技術，至於圖片方面主要利用數位浮水印技術達到防竄改，然現行的機制只能個別保護單一資料來源，不適用於數位典藏環境。

以下各章節的安排順序分別為文獻探討、資料防竄改與資料保護之安全機制、安全性分析與結論。

2. 文獻探討

XML 數位簽章

XML 數位簽章是由 W3C 與 Internet Engineering Task Force (IETF)共同推動[8] 。XML 數位簽章是 XML 安全架構裡最基本的組成元件，它可以在 web services 提供驗證基本數據的可靠度，來對於網路上的每筆交易可靠度進行確認。XML 數位簽章最大的特色是其可以在 XML 文件之部分區段進行簽章，而非僅只能針對整份文件進行簽章。

數位典藏採用之資料格式

數位典藏機構採用許多格式標準，在圖書館書目方面採用MARC(MAchine Readable Cataloging)、在博物館典藏品採用CDWA(Categories for the Description of Works of Art)、在檔案全文方面採用EAD(Encoded Archiral Description)，其中EAD資料格式特別適用於檔案方面的資料建檔，EAD採用Document Type Definition (DTD)為標準

*本研究接受國科會研究計畫案 NSC 94-2422-H-212 -001, NSC 93-2622-E-212-005-CC3 資助，特此致謝。

制定其XML資料格式，由Network Development and MARC Standards Office 所維護，以下即EAD資料格式的範例，在說明Area, Interdisciplinary, and Ethnic Studies -- AfricanAmerican Studies的主題[15]。

```
<ead>
 <eadheader audience="internal" countryencoding="iso3166-1"
dateencoding="iso8601"
 langencoding="iso639-2b" repositoryencoding="iso15511">
  <eadid countrycode="us" mainagencycode="cu-i"
publicid="-//us::cu-i//TEXT us::cu-i::
  p29.sgm//EN">Mildred Davenport Dance Programs and Dance
School Materials, MS-P29
 </eadid>
 <filedesc>
  <titlestmt>
   <titleproper>Guide to the Mildred Davenport Dance Programs
and Dance School
    Materials</titleproper>
   <author>Processed by Adrian Turner; machine-readable
finding aid created by Adrian
    Turner</author>
  </titlestmt>
  <publicationstmt>&hdr-cu-i-spcoll;
   <date>&copy; 2001</date>
   <p>The Regents of the University of California. All rights
reserved.</p>
  </publicationstmt>
  <notestmt>
   <note>
    <p>
     <subject source="cdl">Arts and
Humanities--Dance--Dance Performance
     </subject>
     <subject source="cdl">Arts and
Humanities--Dance--Dance History and
     Criticism</subject>
     <subject source="cdl">Area, Interdisciplinary, and Ethnic
Studies--African
     American Studies</subject>
    </p>
   </note>
  </notestmt>
 </filedesc>
 <profiledesc>
  <creation>Machine-readable finding aid derived from MS
Word. Date of source:
  <date>2001.</date></creation>
  <langusage>Description is in <language>English.</language>
  </langusage>
 </profiledesc>
</eadheader>
…
</ead>
```

圖 1 EAD 範例

數位浮水印

在數位浮水印方面，自從 1950 年代開始，開始有一些研究報告或專利發明[8, 1]，提及了將一些資訊藏入特性訊號（影像、音樂等）內，日後可當作版權所有的證明。近年來的研究，讓數位資料的版權證明與內容正確性驗證，成為影像分析、密碼學等各領域的重要研究課題。隨著數位典藏機構將典藏資料數位化，政府亦鼓勵影像版權技術的研究，以提供完整的版權解決方案。部分學者將密碼學的數位簽章與影像浮水印技術整合，提供另一個方向的應用。Wong[12]利用影像本身的內容的基本資訊，包括編號、影像寬度及高度等公開資訊，先進行單向雜湊函數計算，再利用圖片擁有者私鑰對其簽署數位簽章，最後將此簽章作為浮水印嵌入至影像的空間域（Spatial Domain），此機制的優點在於任意第三者都可以對影像進行認證其完整性及簽署人。但一些易脆式（Fragile）的浮水印認證系統，將無法抵抗影像壓縮及雜訊對浮水印造成的破壞[5]。Lee[6]對影像空間域資訊簽署數位簽章再嵌入之，還使用了錯誤偵錯碼，可以進一步地加強了浮水印的強健性。強調浮水印強韌度的強健式（Robustness）浮水印[7]，主要在於具抗拒試圖移除或破壞浮水印的攻擊行為，包括影像模糊化、影像切割、影像旋轉等影像處理動作都無法破壞或移除浮水印，不過這樣使得我們可以在未損及浮水印的情況下竄改影像內容。另一種解決方案是為半易脆式（Semi-fragile）數位浮水印[13, 14]，此類浮水印系統具有容忍壓縮及非人為惡意破壞行為的能力，對於人為惡意的偽造，竄改等行為可以透過認證來辨識出。

然而，XML 簽章與影像浮水印技術，無法對典藏機構間傳遞的 EAD 檔案與影像附件，達到避免資料竄改的防護機制，原因如下：

1. 在史料影像中加入典藏單位的數位浮水印，此技術只能保護單一的圖片的防竄改，但是一份數位史料是由 EAD 與多個圖檔組成，有心人士只要抽換成該典藏機構的其他圖檔，並且將圖檔修改成相同檔案名稱，所以單純的數位浮水印將無法偵測出這樣的攻擊。
2. EAD 已經是數位典藏的國際標準，如果直接導入 XML 數位簽章，需要修改 EAD 的格式標準，造成與現行閱讀 EAD 的程式不相容。
3. 保護原始 EAD 內容所採用之數位簽章，除保護 EAD 不被竄改外，還需記載數位簽章時的相關資訊，以利後續追蹤之用途，例：簽章姓名、簽章時間、圖檔位置。若這些簽章的相關資訊被竄改，則會無法有效檢查數位史

料，所以數位簽章是需要被嚴格保護。以下將說明數位簽章相關資訊被竄改的嚴重性。竄改簽章人姓名會無法得知是由何人發出簽章進而無法得知使用者公鑰、竄改簽章時間會造成工作程序的爭議、竄改圖檔位置會造成無法得知圖片的相關位置，進而無法找出相對應的圖檔做更完整的浮水印檢查。因此，XML 數位簽章並無法滿足上述需求。

為了解決上述三個問題，有必要發展適用於數位典藏環境的資料保護之安全保護機制，以滿足現行典藏機構之安全需求。本論文具體作法是在利用數位簽章當作浮水印的方式，將數位簽章置入圖檔。另外，EAD 文件與相對應之圖檔透過網路交換亦需提供安全性的保護機制，以防止有心人士將非法 EAD 文件或圖檔內容交換給其他典藏機構。

橢圓曲線密碼系統

由於本機制需要將數位簽章值當成浮水印置入圖片中，然而圖片所能隱藏的資訊量有限，若隱藏的資訊量過大則會破壞圖片之畫質。所以需選擇安全等級高且簽章長度較短的公開金鑰密碼系統，才能安全又有效率的完成後續機制。在公開金鑰密碼系統中 RSA[9]與 ElGamal[1]系統中需要使用 1024 位元的模數，才能達到足夠的安全等級，而 ECC 只需要使用 160 位元的模數即可 [1, 10]，所以本論文以橢圓曲線密碼系統做密碼學之基礎設計相關機制。

橢圓曲線密碼系統是由 Koblitz [4]和 Miller[11]兩位學者所提出來的。在有限場 Fp 之下，給定橢圓曲線 E 上的兩個點 P 及 Q，當點 P 的序(order)夠大時，要找出一個整數 x，使得 Q = x · P 是很困難的，此問題稱為解橢圓曲線離散對數問題(Elliptic Curve Discrete Logarithm Problem；ECDLP)。

3.資料防竄改與資料保護之安全機制

為了設計出適用於 EAD 的資料保護機制，本章將分成系統建置階段、製作數位浮水印階段、EAD 數位簽章階段、數位史料交換階段及數位史料驗證階段分別探討。

3.1 系統建置階段

參數定義：

$E: y^2 = x^3 + ax + b\,(x, y, a, b \in \mathrm{F}_p)$的點$(x, y)$所構成的集合

p：大質數(使得點 P 存在)。

q：p - 1 的質因數，長度 160 位元。

h：單向雜湊函數(One-way hash function)。

E：橢圓曲線方程式。

$E(\mathrm{F}_p)$：在 F_p 之下，E 上全部的點所構成的集合。

P：序為 q 的點。

E, p, q：系統的公開參數。

$d \in [2, q-2]$：使用者的私鑰。

$Q = dP \bmod p$：使用者的公鑰。

DA：數位典藏機構。

DA_KR：數位典藏機構之私鑰，生成方法如 d。

DA_KU：數位典藏機構之公鑰，生成方法如 Q。

SDA：資料交換時，來源端的數位典藏機構。

DDA：資料交換時，目地端的數位典藏機構。

$FileID$：數位史料的編號，可以在不同數位典藏機構間識別不同的數位史料。

EAD_{FileID}：數位史料編號為 FileID 的 XML 檔，其合乎 EAD 格式規範。

SIG_{FileID}：數位史料編號為 FileID 的數位簽章。

$IMG_{FileID,i}$：數位史料編號為 FileID 的第 i 份影像檔。

$W_{FileID,i}$：數位史料編號為 FileID 的浮水印內容。

V_{DA_KU}(data, signInfo)：檢驗 XML 數位簽章是否正確，其中 DA_KU 為公鑰、data 為原始資料內容、signInfo 為數位簽章值。

XQuery(xpath)：以 xpath 查詢 XML 資料的節點之內容。

||：字元串接符號。

產生公開金鑰：

首先，各數位典藏機構 DA 利用公開金鑰密碼系統，選定其私鑰 DA_KR，並生成其公開金鑰 DA_KU。該數位典藏機構的管理者保管 DA_KR，並將 DA_KR 視為該典藏機構的機密，並公開 DA_KU 給其他典藏機構及社會大眾。

製作史料文件：

假設數位典藏機構 DA 已經製作許多史料文件，並且制定其史料編號 $FileID$，並且擁有 EAD_{FileID} 檔案及其相對應的數份的 $IMG_{FileID,i}$，其中 $1 \le i \le n$，n 為該文件之

圖片總份數，這此數位史料都是待公開的內容。

3.2 製作數位浮水印階段

以下是將版權資料置入史料圖片的運流程：

1.首先將計算下列版權資訊

$$W_{FileID,i} = Sig_{DA\_KR}(FileID \| i)$$

2 利用隱藏式數位浮水印機制，將 $W_{FileID,i}$ 置入史料圖片，其觀念如圖 2 所示，其中(a)為未嵌入浮水印的原始影像，將 $W_{FileID,i}$ 嵌入後成為已加入浮水印的影像。

針對以上兩步驟特舉例如下，其中圖 2(a)尚未加入數位浮水印，加入浮水印簽章資料（$W_{FileID,i}$）之後，則如圖 2(b)所示。

(a)

(b)

圖 2 將浮水印置入圖片

3.3 EAD 數位簽章階段

在 EAD 數位簽章階段，採用系統建置階段時生成之 DA_KR，一份史料的 EAD 檔案進行下列運算:

$$imageInfo = W_{FileID,1} \| W_{FileID,2} \| ... W_{FileID,n}$$

$$fileInfo = FileID \| time \| organization \| userName$$

$$SIG_{FileID} = Sig_{DA\_KR}(EAD_{FileID} \| fileInfo \| imageInfo)$$

將 $fileInfo$ 及 SIG_{FileID} 以XML註解方式加入至 EAD_{FileID} 中，實作上則如圖 3 所示，由於XML中以「<!-- 註解內容 ➔」當做為註解之用途，所以一般XML之解析器不會對此段內容做解析，在執行本機制時再特別解析此此註解，將其內容視為可讀的XML即可，此做法最大的好處在於能與現行閱讀EAD檔案的程式相容，不會因為增加數位簽章而需修改EAD標準，達到向下相容的好處。類似的作法在W3C組織將HTML導入JavaScript 及 CSS語法時，亦採用類似作法，所以本做法可以被實作，而且可以與現行EAD格式相容，如圖 3 所示。

```
<EAD>
  …原始 EAD 內容…
</EAD>
<!--
<signature>
   <fileInfo>
      <fileID>0007-001</fileID>
      <time>2005/6/18 00:00:00</time>
      <oranization>國史館臺灣文獻館</oranization>
      <userName>林大立</userName>
      <version>2005/6/18</version>
   </fileInfo>
   <imageInfo>
      <image index=”1” filename=”pic01.jpg” />
      <image index=”2” filename=”pic02.jpg” />
      <image index=”3” filename=”pic03.jpg” />
   </imageInfo>
   <signature>
      …對\EAD 及 signature\fileInfo 的 ECC 數位簽章值
   </signature>
</signature>
-->
```

圖 3 以註解方式加入 EAD 之數位簽章

3.4 數位史料驗證階段

欲檢驗一份 EAD 文件及其相對應的圖片是否正確，其演算法如下。其做法預計此 EAD 內容是正確的，逐一檢查各個項目，當發現錯誤則結束演算法並回傳錯誤訊息。

演算法 CheckEAD
輸入參數：EAD_{FileID}
輸出結果：此 EAD 及其圖檔是否正確。若正確則回傳"Success"
否則回傳錯誤訊息。

EAD_SIG = EAD_{FileID} 中被 XML 註解的版權資料
//檢查 EAD 是否有含版權資料，無版權資料則離開
if(EAD_SIG is Empty) return "Reject:無版權資料"

eadInfo = XQuery(EAD_{FileID} \ead)
fileInfo = XQuery(EAD_SIG\fileInfo)
imageInfo = XQuery(EAD_SIG\imageInfo)
sigInfo = XQuery(EAD_SIG\signature)

data = eadInfo || fileInfo || imageInfo
if(V_{DA_KU}(data, signInfo) $\stackrel{?}{=}$ False) return "Reject:簽章錯誤"

fileID = XQuery(fileInfo@file_id)
for item in XQuery(imageInfo\image)
  name = XQuery(item@filename)
  img = OpenImage(imgFileName)
  $W_{FileID,i}$ = img 之浮水印 //即事先置入之版權資料
  rightW = V(fileID||XQuery(imageInfo@index), $W_{FileID,i}$)
  if(rightW $\stackrel{?}{=}$ False) return "Reject: Image Error " || name
next
return "Success"

圖 4 檢驗 EAD 簽章之演算法

3.5 數位史料交換階段

數位典藏機構共同制定 EAD 格式，其主要目地在於能讓數位史料文件有共同的交換格式，增加史料文件的互通性，因此本機制亦以史料文件交換為探討對象。當兩個數位典藏機構要進行資料交換，資料發送端稱 SDA，資料接收 DDA。SDA 將發送 EAD 檔案及其圖檔給 DDA。然典藏單位為求圖片具高解析度，所以其檔案大小較大，為了節省網路的通訊成本，在交換資料時應以 EAD 與圖檔版本判斷是否需要傳輸內容，詳細內容如下：

1. SDA選定要傳輸檔案EAD_{FileID}與目地端DDA。
2. SDA 與 DDA 建立 socket 連線。
3. SDA 傳送 FileID 與 version 給 DDA。
4. DDA 查看此 FileID 的 EAD 文檔是否已經存在 DDA 系統，若不存在則接受此傳輸，否則再判斷 EAD 文檔的 version 是否比現行文檔舊，若是現行版本較舊則接受交換，否則拒絕傳輸。這樣的做法可以避免不必要的傳輸與檢驗。
5. DDA 根據步驟 4 的結果，回應 SDA 是否願意接受檔案。
6. 若 SDA 願意接受檔案，則將 EAD_{FileID} 傳送給 DDA。
7. DDA 將收到的 EAD_{FileID} ，將 XQuery(EAD_{FileID})結果送交演算法 CheckEAD 檢查。其中若需要圖檔時，執行下列演算法進行取得與檢查。

for item in XQuery(imageInfo\image)
  name = XQuery(item@filename)
  img = OpenImage(imgFileName)
  $W_{FileID,i}$ = img 之浮水印 //即事先置入之版權資料
  rightW = V(fileID||XQuery(imageInfo@index), $W_{FileID,i}$)
  if(rightW $\stackrel{?}{=}$ False) return "Reject: Image Error " || name
next

8.完成相關交換與檢驗，儲存 EAD 資料與圖檔。

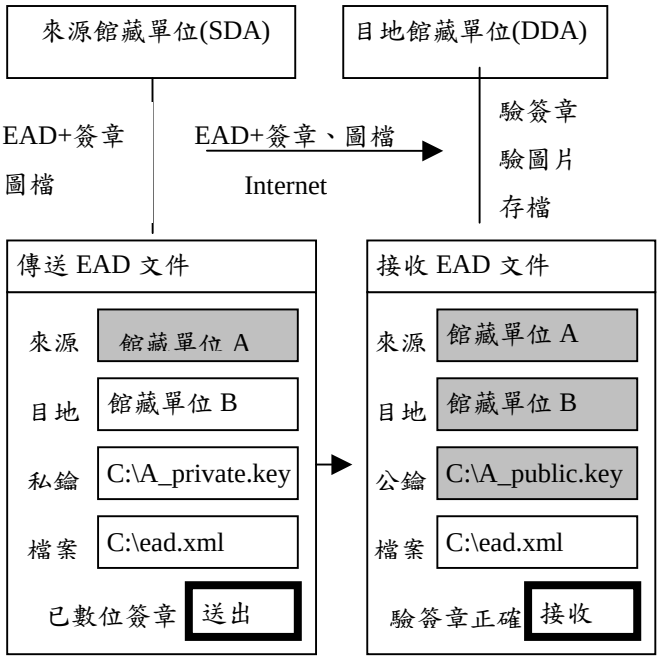

圖 5 位史料交換示意圖

4 安全性分析

本機制主要整合 ECC 之數位簽章與數位浮水印的優

點，完成機制的設計。

假設條件

1.只有典藏機構擁有 DA_KR，其他使用者均無法得知。
2.企圖攻擊者，可以讀取、修改、置換任意 EAD 檔案及其圖檔。
3.當使用者檢驗 EAD 及圖檔時，若本機制無法偵測出內容遭受竄改則表示攻擊成功，否則攻擊失敗。

我們模擬惡意使用者，可以採用下列幾項攻擊方式進行。

攻擊 1：偽造 EAD 文件

攻擊者試圖偽造一份不存在的 EAD 文件、竄改數位簽章或竄改 EAD 文件時，由於無法取得 DA_KR，只能使用 DA_KR' = random 進行數位簽章。然而在演算法 CheckEAD 中執行至下列驗簽章程序時，攻擊會被偵測。

$\text{if}(V_{DA\_KU}(\text{data}, \text{signInfo}) \stackrel{?}{=} \text{False})$ return "Reject:簽章錯誤"

攻擊 2：竄改圖檔

攻擊者偽造或竄改一份圖檔時，由於無法取得 DA_KR，只能使用 DA_KR' = random，因此其無法正確產生 $W_{FileID,i} = Sig_{DA\_KR}(FileID \| i)$，即使用 DA_KR' 完成簽章，在 CheckEAD 演算法中計算列式函式。

rightW = V(fileID||XQuery(imageInfo@index), $W_{FileID,i}$)

計算結果 rightW 結果必為 False，其竄改圖檔的行為，在下列判斷式將會被偵測出攻擊。

if(rightW $\stackrel{?}{=}$ False) return "Reject: Image Error " || name

攻擊 3：竄改 EAD 文件中圖檔位置

攻擊者將 EAD 文件中圖檔閱讀順序調換或刪除。由於 EAD 文件是連同影像的簽章資訊均被數位簽章保護，EAD 數位簽章階段中，圖片的檔名及其順序(*imageInfo*)，都被數位簽章保護，其計算式如下：

$$SIG_{FileID} = Sig_{DA\_KR}(EAD_{FileID} \| fileInfo \| imageInfo)$$

本攻擊在數位史料檢驗階段的下列演算法會偵測錯誤

data = eadInfo || fileInfo || imageInfo

$\text{if}(V_{DA\_KU}(\text{data}, \text{signInfo}) \stackrel{?}{=} \text{False})$ return "Reject:簽章錯誤"

因此，本機制不會面臨圖檔閱讀順序被調換或刪除的問題。

攻擊 4：抽換浮水印

針對某 FileID 的圖檔，攻擊者試圖用典藏機構的其他有浮水印的圖檔來取代，在先前學者的做法只能驗證此圖檔是否屬於此典藏機構發現，但無法知道此圖檔屬於那個文檔。而在本機制中由於 EAD 文件是連同影像的簽章資訊均被數位簽章保護，EAD 數位簽章階段中，圖片的檔名及其順序(*imageInfo*)，都被數位簽章保護，其計算式如下：

$$SIG_{FileID} = Sig_{DA\_KR}(EAD_{FileID} \| fileInfo \| imageInfo)$$

本攻擊在數位史料檢驗階段的下列演算法會偵測錯誤

data = eadInfo || fileInfo || imageInfo

$\text{if}(V_{DA\_KU}(\text{data}, \text{signInfo}) \stackrel{?}{=} \text{False})$ return "Reject:簽章錯誤"

因此，本機制不會面臨圖檔閱讀順序被調換或刪除的問題。

攻擊 5：傳送非法的 EAD 或圖檔

攻擊者試圖利用數位史料交換將遭竄改或偽造的資料傳輸給數位典藏機構。

由於本研究在交換階段會檢驗 EAD 的數位簽章、圖片的浮水印及 EAD 與圖檔的關聯，所以前述第 1, 2, 3, 4 的攻擊手法，在交換階段亦不會發生。

攻擊 6：舊版資料取代新版資料

數位史料製作過程，對相同的數位史料會因為 EAD 資料更新而採用新的 EAD 文件。並讓舊有的版本廢除，因此若攻擊者用舊的數位史料給予交換，則在數位史料交換階段的步驟 4，會被偵測出來。

我們將以上六種常見的攻擊手法與現行「XML 數位簽章」、「數位浮水印」、「同時導入 XML 數位簽章、浮水印」與「本機制」的安全性作一比較，如表 1 所示。

由表 1 對於各項攻擊的比較，可以得知本機制較現行的機制能偵測為佳，其主因為在先前做法史料影像中加入典藏單位的數位浮水印，此技術只能保護單一的圖片的防竄改，但是一份數位史料是由 EAD 與多個圖檔組成，若有心人士將某圖檔抽換成相同典藏單位但屬於不同文件

的其他圖檔，則單純的數位浮水印將無法偵測出這樣的抽換影像攻擊，而本機制能確實偵測抽換影像攻擊。

在資料傳輸的機密性方面，由於本機制運作在 TCP/IP 的應用層，因此可以與現行的 Secure Socket Layer(SSL) 相容，或者採用 XML 的加密機制，均可達到傳輸的機密性。

表 1 安全性之比較表

比較項目	XML 數位簽章	數位浮水印	簽章與浮水印	本機制
攻擊 1	○	╳	○	○
攻擊 2	╳	○	○	○
攻擊 3	╳	╳	╳	○
攻擊 4	╳	╳	╳	○
攻擊 5	╳	╳	╳	○
攻擊 6	╳	╳	╳	○

註 1：「○」能偵測，「╳」無法偵測。

註 2：簽章與浮水印指同時導入現行 XML 數位簽章與數位浮水印兩項機制。

5 結論

由於數位典藏機構的史料文件由 EAD 文件與圖檔共同組合而成，本研究針對 EAD 文件與圖檔關聯，設計出 EAD 檔案與圖檔的保護機制。而且本研究針對史料文件透過網路交換亦提供安全性的保護。因此本機制能偵測出非法竄改或惡意偽造而成的 EAD 與圖檔。以具體保護數位典藏機構之資料安全，間接保障典藏機構之名譽。因此本研究適用於數位典藏機構。

本機制除能有效應用於數位典藏機構外，亦可將本研究推廣於其他類似擁有資料與圖檔有關聯性的場合，不只能各別保護資料與圖檔之防竄改，還能確保資料與圖檔的關聯性不被惡意破壞。例如：在醫學方面，醫院的 XML 病歷與其醫療影像。在網路新聞方面，將 XML 格式的 RSS 與其新聞照片、在網路方面，產品資訊與產品圖片。

參考文獻

1. W. Caelli, E. Dawson, and S. Rea, “PKI, elliptic curve cryptography and digital signatures,” *Computer & Security*, Vol. 18, No. 1, 1999, pp. 47-66.
2. T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Transactions on Information Theory*, Vol. IT-31, No. 4, 1985, pp. 469-472.
3. E.F. Hembrooke, “Identification of sound and like signals,” *United States Patent*, 3,004,104, 1961.
4. N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of Computation*, Vol. 48, No. 17, 1987, pp. 203-209.
5. T. Liu and Z. D. Qiu, “The Survey of Digital Watermarking-based Image Authentication Techniques,” *Signal Processing*, vol. 2, pp. 1556-1559, 2002.
6. J. Lee and C.S. Won, “A Watermarking Sequence Using Parities of Error Control Coding for Image Authentication and Correction,” *IEEE Transactions on Consumer Electronics*, vol. 46, no. 2, pp. 313-317, 2000.
7. C.Y. Lin, M. Wu, J.A. Bloom, I.J. Cox, M.L. Miller and Y.M. Lui, “Rotation , Scale and Translation resilient watermarking for images,” IEEE Transactions on Image Processing, vol. 10, no. 5, 2001.
8. W.M. Tomberlin, L.G. MacKenzie, and P.K. Bennett, “System for transmitting and receiving coded entertainment programs,” *United States Patent*, 2,630,525, 1953.
9. R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120-126.
10. S. Vanstone, “Elliptic curve cryptosystem - the answer to strong, fast public-key cryptography for securing constrained environments,” *Information Security Technical Report*, Vol. 2, No. 2, Elsevier, 1997, pp. 78-87.
11. V.S. Miller., “Use of elliptic curves in cryptography,” *Advances in Cryptology:Crypto’85*, Springer-Verlag,1986, pp. 417-426.
12. P. W. Wong and N. Memom, “Secret and Public Key Image Watermarking schemes for Image Authentication and Ownership verification,” *IEEE Transaction on Image Processing*, vol. 10, no. 10,

2001.
13. C.W Wu, “On the Design of Content-Based Multimedia Authentication System,” *IEEE Transaction on Multimedia*, vol. 4, no. 3, 2002.
14. F.Y. Shih and S.T. Wu, “Combinational Image Watermarking in the Spatial and Frequency Domains,” *Pattern Recognition Letters*, vol. 36, no. 4 , pp. 969-975.
15. Encoded Archival Description (EAD), <http://www.loc.gov/ead/>, 2002.
16. W3C XML Signature, <http://www.w3.org/Signature >, 2001.