

# A Model of Unforgeable Digital Certificate Document System

Koichi Nozaki<sup>\*</sup>, Hideki Noda<sup>\*\*</sup>, Eiji Kawaguchi<sup>\*\*</sup> and Richard Eason<sup>\*\*\*</sup>  
<sup>\*</sup>Nagasaki University, <sup>\*\*</sup>Kyushu Institute of Technology, <sup>\*\*\*</sup>University of Maine  
(\* nozaki@net.nagasaki-u.ac.jp, \*\*{noda, kawaguch}@know.comp.kyutech.ac.jp)

**Abstract.** Certificate documents today are either written or printed matter on a paper surface or plastic card. No digital data are accepted as a certificate document. People always asked to send an original certificate documents by traditional post mail even in this developing information age. The present paper proposes an unforgeable certificate document system wherein each document has a forgery-protective capability by itself. It does not need any communication with an authentication bureau. The system has several variations according to the key usage and additionally incorporated data. If this system is implemented, all certificate documents may be digitalized.

## 1. Introduction

Almost all documents nowadays are handled in a digital manner except for one very important case. It is the certificate document. Today, an authentic certificate document, that is original, cannot take a digital form. Certificate documents must be either written or printed on a paper surface or on a plastic card. For example, a driving permit or passport is always a printed matter. No digital data work as a driver's license, or a passport. All current certificates consist of information data and a base substance on which the information data is located. The base substance itself does not have any meaning. It only carries the information.

The reason why a digital document is not accepted as a certificate is very obvious. All digital documents currently used are easily forged without leaving any clues for forgery detection. No one has any means to tell whether a given digital document is authentic or not.

Printed matter is believed to be much more secure, or more difficult to forge, than digital data because the printed information is generally difficult to erase and change, and the state of the art printing techniques to defy attempts to forge documents have been developed every day. Handwritten matter, e.g., a signature, is also regarded as a difficult-to-forged document because mimicking someone's hand writing skill and habits is not an easy task for an ordinary person. So, a certificate document often carries a signature made by an authorized person in such a way that it is difficult to separate it from the document information.

In the meantime, with the advent of the information age there is a surge of demand among people in the world that the certificate documents can be also handled in a digital manner. People hope to send and receive certificates through the Internet. The reality, however, is that people still send and receive paper certificates by way of traditional post mail with high cost.

In this situation, an invention of an unforgeable digital document system is long awaited. If invented, digital data could work as a certificate document by itself, and transmitted to any place in the world through the Internet. Currently, there are “signature certification” systems that use a public-and-private key system [1]. However, these systems need time and cost on the user’s side. This makes them unsatisfactory for everyday use.

## **2. Document forgery**

Document forgery is classified into two following categories.

- (1) Type-1 forgery: Altering a part of an authentic certificate that is original
- (2) Type-2 forgery: Producing a new fake certificate with false information

Type-1 forgery occurs when some part of the original document is altered to benefit someone who is not benefited by the original document. In this case the base substance, such as a paper sheet or plastic card, is legal and valid, but the information contained is forged. For example, a stolen photo credit card may be altered by replacing the photo picture on the card, the expiration date on a drivers license could be altered to make it still valid after the original license expires, the grading scores on a student report card may be changed from C’s and D’s to all A’s, etc.

Type-2 forgery is the case when both the base substance and the information data are false, but it is hard to tell if it is genuine or fake because the base substance and the style of the document look very authentic. Most passport forgeries belong to this category. Type-2 forgeries include attempts to create authentic looking, but false, information data.

The most important aspect of the Type-2 forgery is as follows. Forging is always targeted at a certificate document that is issued by a high authority, such as the government of a country, a public organization, world known big business, or a very famous person in the world. While, a certificate issued by an average citizen, or un-trusted company, are seldom forged. This is because people regard a high authority as simply trustworthy without any authentication. Once a high authority have announced or published something, people trust it as it is. The high authority itself automatically serves as an authentication bureau.

An “unforgeable document” should satisfy the following conditions.

- C-1 A forged document has some difference from an authentic original document in some way
- C-2 The forgery detection can be done without referring to the authentic original document
- C-3 There is a concrete verification method that detects a forged document without communicating with an authentication bureau.

If a system can produce such a digital document that satisfies all these conditions, the system is titled as an unforgeable digital document system. An “unforgeable digital certificate document system” is an

unforgeable digital document system that is used for a certification system.

### 3. Information structure in the current digital document

Documents consist of characters, digits, tables, illustrations, photo pictures, etc. Its digital version, i.e., digital document, is a computer file. Digital documents are designed to produce visual information on the computer monitor. Therefore, every digital document can take an image form rather than a combination of the different file types (e.g., one “BMP” file instead of the combination of “WORD”, “JPEG” and “EXCEL” files) if the overall visual information is the same.

A current digital document has a single-layered information structure in the sense that all information is just as it looks. No hidden information is included in the document. So, it is quite easy to alter the original document using a text editor or an image editor. It is also easy to produce an entirely fake document that looks very authentic by using computers. Nobody can tell whether a given digital document is authentic or not.

Therefore, an unforgeable digital document, if ever exists, cannot take a single-layered information structure. Instead, it should have “a multi-layered” information structure having the following properties.

- (A) The information data on both the external and internal layer are tightly linked.
- (B) The internal information is not extracted without a special means to extract.
- (C) The internal information is not changeable as attempted.

Fig. 1 illustrates a concept of the single-layered document and the corresponding multi-layered document.

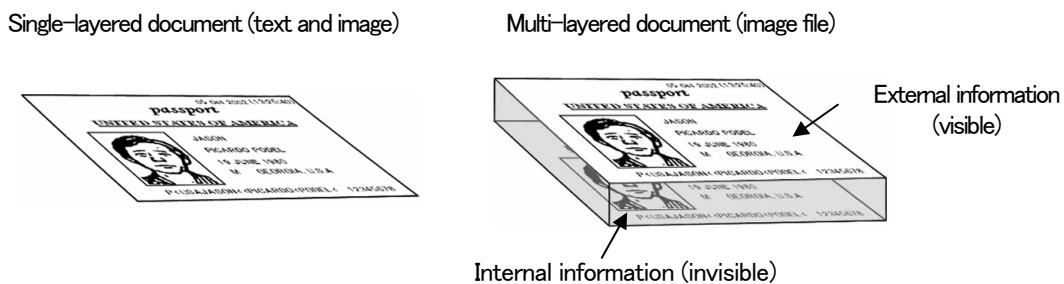


Fig. 1 A single-layered and a multi-layered document

In this example the multi-layered document is an image data, and the external and the internal information is the same as the original single-layered document information. Once someone has altered the external layer by using an image editor, there occurs some discrepancy between the two layers. Or, the internal information is significantly disordered.

#### 4. How to implement a multi-layered information structure

We know that a steganographic technique can implement a multi-layered information structure in an image data by using an embedding program. The external layer in that case is the visual information of the original document, which is the cover image in steganography, and the internal layer is the embedded information. If we embed the original document in the internal layer, we will get a multi-layered information structure as is shown in Fig. 1.

A BPCS-Steganography [2] [3] is a good method for this purpose because the embedding capacity is very large and the embedded data is quite fragile. Fig. 2 shows a data embedding procedure by steganography in general. An embedding program is used for embedding, an extracting program is used for extracting the embedded information.

Fig. 3 illustrates a scheme to create a multi-layered digital document from an original document. In this procedure the Document Image data becomes larger than the original document in size.

As the internal information is not changeable as attempted, any alterations on the external layer can be detected by comparing with the internal layer. If both meet, the document is authentic otherwise the document is forged.

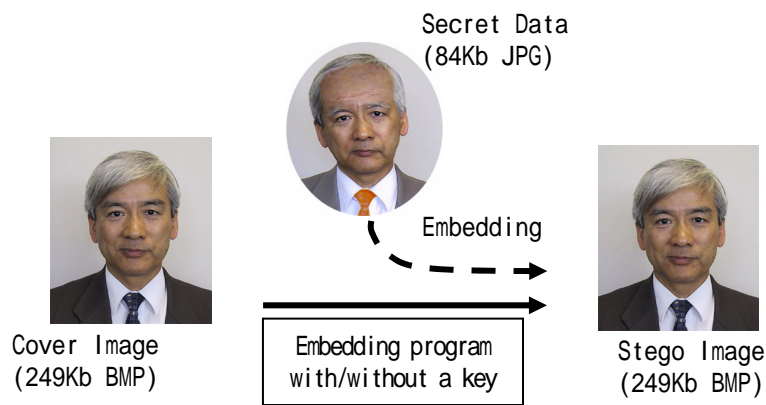


Fig. 2 Data embedding by steganography

Secret data is embedded in the cover image to get the stego image. There is no visible degradation in the stego image. Extracting the embedded data is executed by an extracting program with/without a key.

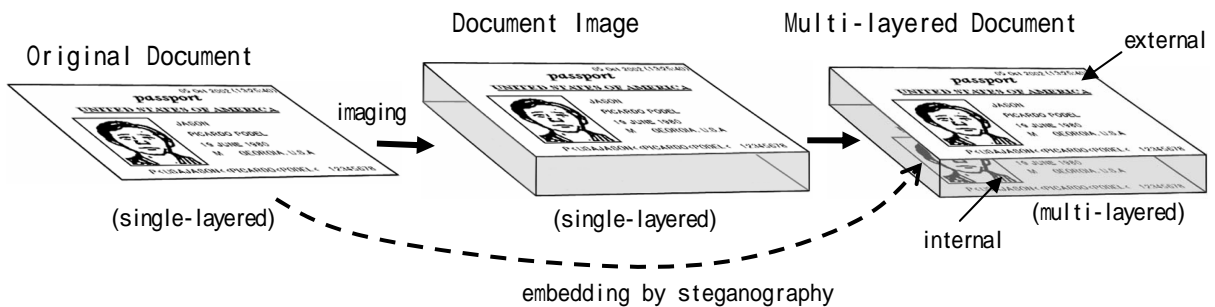


Fig. 3 Multi-layered document production procedure

## 5. Unforgeable digital certificate systems

As we have shown in Fig. 3, the multi-layered digital image is the basic structure of the unforgeable digital document. It has some variations according to the functions in the document producer and the key in the system as well as other incorporated data.

### 5.1 Type-1 system: A Type-1 forgery protective system

Type-1 system consists of the Document Producer and the Document Verifier. The system can only detect whether the document was altered or not after it was created. It does not matter if the document is a certificate or a general document.

Fig. 4 (a) illustrates the flow diagram of the Document Producer of Type-1. The input to the system is an Original Digital Document ( $Doc_{org}$ ). The output is the Multi-Layered Digital Document consisting of the external and the internal information, i.e.,  $Doc=(Doc_{ext}, Doc_{int})$ . We call a Type-1 multi-layered document a Type-1 document.

While, Fig. 4 (b) shows the flow of the Type-1 Document Verifier. A Type-1 forgery on a Type-1 multi-layered document is easily detected by this Document Verifier.

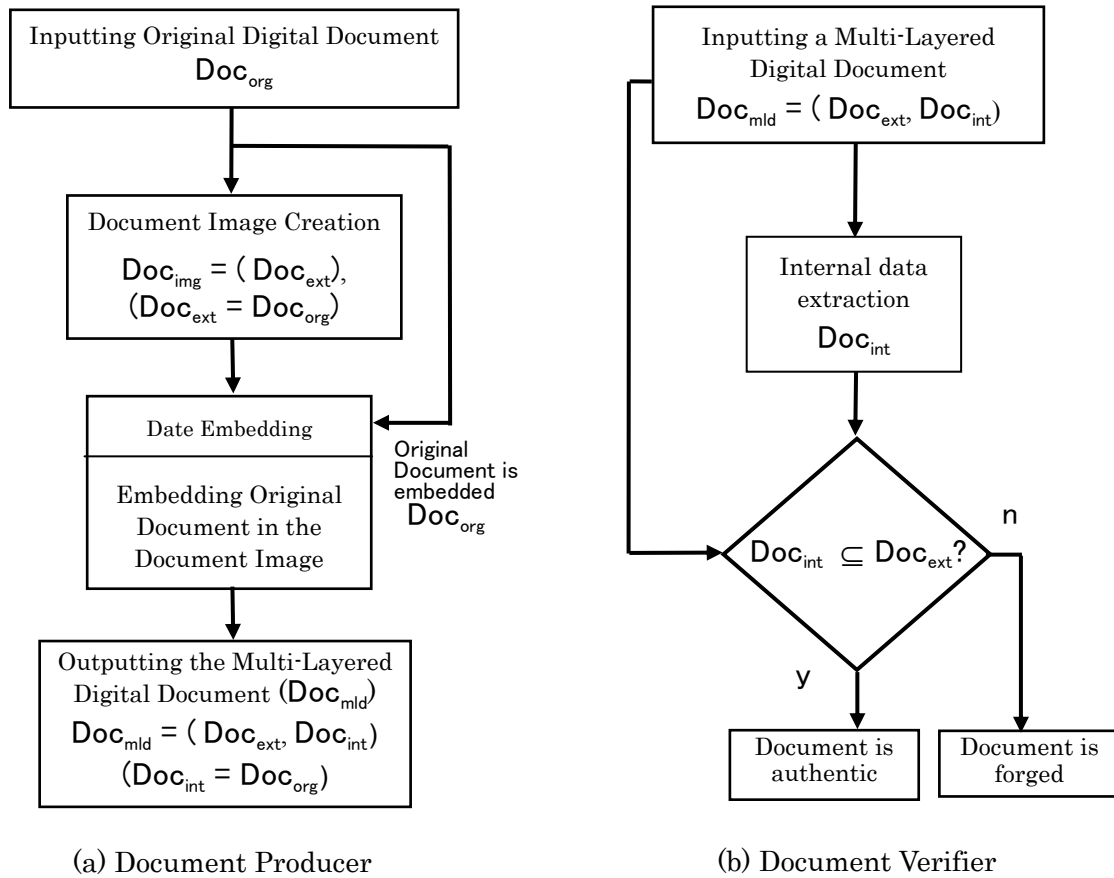


Fig. 4 Type-1 digital unforgeable document system

## 5.2 Type-2 system: A Type-2 forgery protective system

A type-2 forgery is attempted on a certificate document issued by a high authority, which needs no authentication by a third party. Passport forgery is a typical example of this forgery type.

A Type-2 system consists of a Type-2 Document Producer and an associated Document Verifier. A Type-1 system is extended to a Type-2 system by incorporating a pair of keys, namely, a Document Production Key ( $K_p$ ) and a Document Verification Key ( $K_v$ ).  $K_v$  is produced from  $K_p$  according to a one-way scrambling function in an unseen manner within the system.

A Type-2 Document Producer works as follows.

First, a document production key ( $K_p$ ) is arbitrarily selected. It is inputted to the system and scrambled one-way to create a document verification key ( $K_v$ ). This  $K_v$  is outputted from the system, and opened public. It is used when the document is verified in the Document Verifier. The document production key ( $K_p$ ) must be kept secret. It is a type of a private key.

Actually,  $K_v$  is confidentially used for embedding the Original Document ( $DOC_{org}$ ) in the Document Image ( $DOC_{img}$ ) to produce the multi-layered document ( $DOC_{mlt}$ ).

However, the key scrambling and the document embedding operations in this Document Producer are unseen from the outside. The key-scrambling and the document embedding are made inseparable in the program. The system is made in a reverse-engineering-protective manner.

Therefore,  $K_p$  works as if it is the key to embed the document, even if  $K_v$  is actually used. We call a Type-2 multi-layered document a Type-2 document.

A Type-2 Document Verifier works as follows.

A Type-2 multi-layered document data is first inputted to the system. The document verification key ( $K_v$ ) is also provided to the system. Then the internal information is extracted in the system and compared with the external information. If both meet, the document is authentic, otherwise forged.

The reason why a Type-2 certificate document is unforgeable is obvious. Someone who tries to forge a Type-2 document must create a document that can be verified by the  $K_v$  that has been opened public by the certificate issuing authority. The only way the forger can succeed is that he must steal the  $K_p$ . However, it is securely kept secret by the authority. Therefore, as long as  $K_p$  is at the certificate issuer's hand, the certificate can never be forged.

The important point in the Type-2 system is that the system uses a pair of keys ( $K_p$  and  $K_v$ ). The basic idea is the same as the traditional "public-key and private-key" system. However, The system here does not need any authentication bureau. The difficulty of detecting  $K_p$  from  $K_v$  is based on both the reverse-engineering protectiveness of the system and the one-way scrambling function. Therefore, the technique to make the system difficult to reverse-engineer (e.g., obfuscation of the program source code) is quite important. The theoretical evaluation of the system security is difficult, but it is practically very secure, or we can make it very safe by many programming techniques.

### 5.3 Type-3 system: An extension of the Type-2 system

A Type-2 system is upgraded by incorporating other information data. Some document in some case needs to be verified the time of document production. In some other case it might be better or necessary to carry information about the geographical location of the document production. Such additional information must not be changed after the document was created.

The time data is acquired by a Network Time Protocol Server (NTP Server) through the Internet. It is quite accurate timing system. We describe this data by TS. In some situation the time data is also obtained from the Radio Standard Time Broadcasting system that is commonly available in many countries today.

As for the geographical location data, the Global Positioning System (GPS) gives us very detailed Latitude-and-Longitude data all over the world. We designate such positioning data by GP.

The document production time and place data (TS and GP) is the data that are unique to each document. No two documents can have the same data if they are included in the document. We call a Type-2 system with TS and/or GP data a Type-3 system. TS and GP are added to the original document. They are placed both external and internal layers of the document image. Fig. 5 (a) illustrates the flow of a Type-3 Document Producer. While, Fig. 5 (b) is the corresponding Document Verifier.

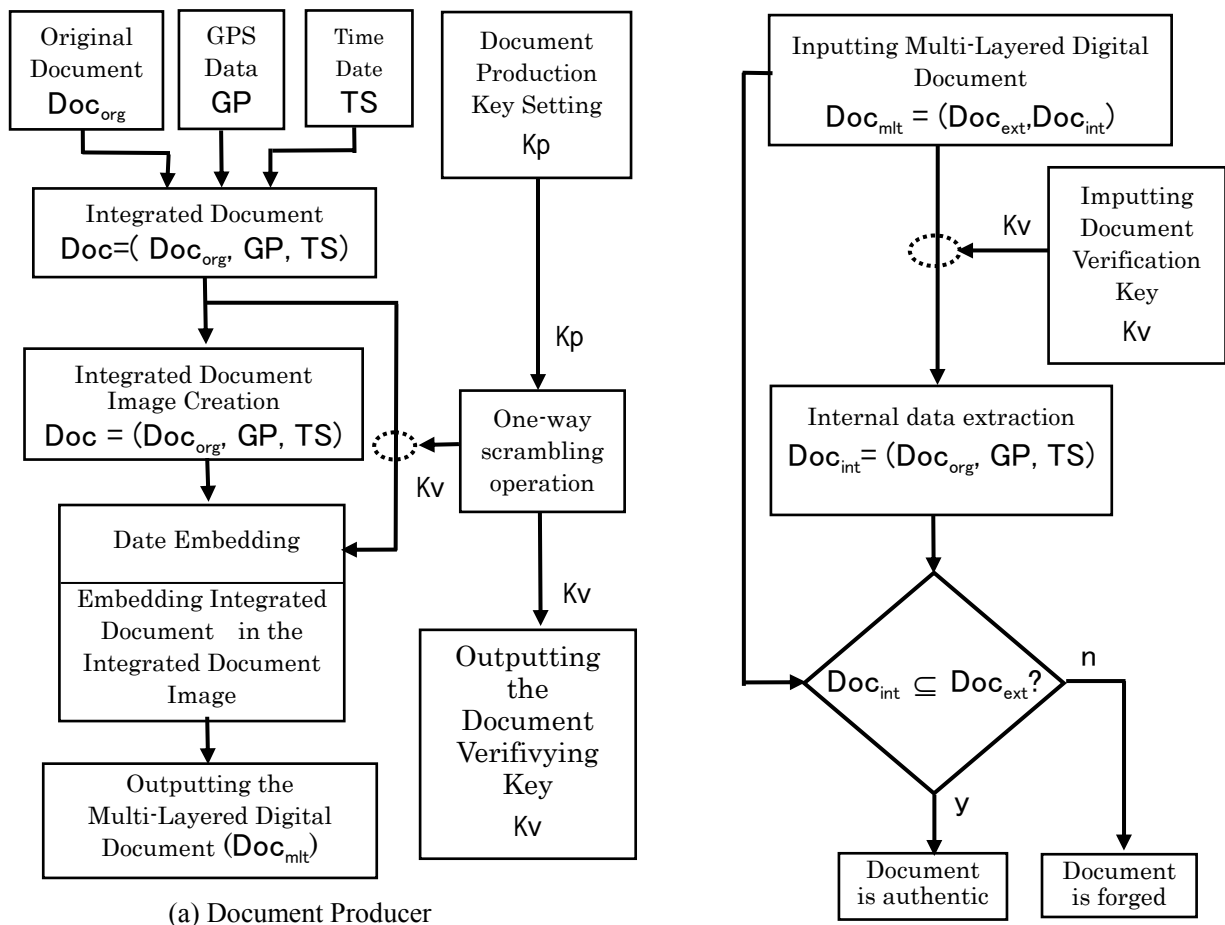


Fig. 5 Type-3 digital unforgeable document system

## 6. Practical applications of the unforgeable certificate system

We will show two example applications here.

### 5.1 Digital passport system

Fig. 6 shows a model of a digital passport. The unforgeable passport data is stored in the IC memory that is mounted on the passport card. The printed information on the card shows the passport information in the IC, but is not the primary data. Rather, it is secondary data just for human eyes. Forgery detection is executed locally at the airport immigration inspection booth in an off line manner. The data in the IC memory can be personally used for sending authorized passport information to remote place through the Internet.

### 5.2 Digital camera system

Fig. 7 illustrates a digital photo picture with the TS and GP data at the top and the camera model date at the bottom.

The photo is verified by the key that is provided by the camera maker (or located at the “Danon’s home page”). If the internal picture is the same as the external, it is an original picture, otherwise a tampered picture. No one can modify this picture without causing damage on the internal picture. This may be very good for many forensic purposes.

## 7. Conclusions

We showed an unforgeable digital certificate document system based on the steganographic technique. If this system is realized, digital sending and receiving of certificate document become very easy and secure. The authors have started working on implementing a prototype system.

## References

- [1] [http://www.murdoch.edu.au/elaw/issues/v9n3/lim93\\_text.html](http://www.murdoch.edu.au/elaw/issues/v9n3/lim93_text.html)
- [2] Koichi Nozaki, Michiharu Niimi, et al “A large capacity steganography using color BMP images”, Proceedings of ACCV’98-Third Asian Conference on Computer Vision, pp.16-23, 1998.
- [3] Eiji Kawaguchi and Richard Eason, “Principle and application of BPCS-Steganography”, Proceedings of SPIE Multimedia Systems Applications, Vol.3528, pp.464-473, 1998.

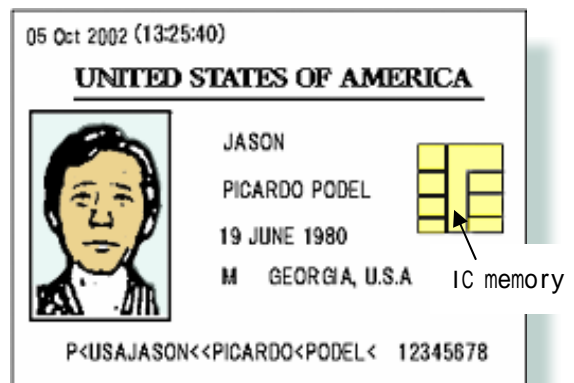


Fig. 6 Digital passport



Fig.7 Unforgeable digital photo