RC 21910 (98544) 13 December 2000 **Computer Science**

IBM Research Report

Application of Invisible Image Watermarks to Produce Remotely Printed, Duplication Resistant, and Demonstrably Authentic Documents

Gordon W. Braudaway, Fred Mintzer, John M. Socolofsky*, Chai Wah Wu
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

*IBM Global Services
Cranford, NJ 01016

Research Division
Almaden - Austin - Beijing - Haifa - T. J. Watson - Tokyo - Zurich

Application of Invisible Image Watermarks to Produce Remotely Printed, Duplication Resistant, and Demonstrably Authentic Documents

Gordon W. Braudaway[a], Fred Mintzer[a], John M. Socolofsky[b] and Chai Wah Wu[a]

[a] IBM Corporation, Thomas J. Watson Research Center, Yorktown Heights, New York 10598
[b] IBM Global Services, Cranford, NJ 07016

ABSTRACT

A secure Internet infrastructure and IBM image watermarking technology have been integrated for the production and authentication of duplication-resistant hard copy documents that may be transmitted to remote sites before being printed. Envisioned applications include the issuance of certificates, contracts, public records, receipts, coupons, ... even college transcripts.

Before issuing a document requested over a secure Internet connection, the unique textual content of the document and identifying information of the paper on which it will be printed are hashed using a secret cryptographic key, known only to an issuing authority, to produce a secure Message Authentication Code (MAC). A derived key produced from the MAC is used to generate a unique texture pattern, called an image watermark. The watermark is then imbedded into an image of the document by modulating the brightness of its pixels. Lastly, the image is compressed and transmitted to a remote ink-jet or laser color printer.

Later, document authentication is accomplished by scanning the printed document and transmitting the compressed scanned image to the issuing agent over the Internet. The agent then extracts the unique textual information using OCR, recalls the appropriate secret cryptographic key, and reconstructs the MAC and the derived watermarking texture pattern. Detection of the derived watermark texture in the received image authenticates document content with a probability approaching certainty. If the unique textual information had been changed, we note, the rebuilt MAC would also have changed and the rebuilt derived watermark texture would differ from the inserted watermark texture. In this case, the rebuilt derived watermark texture would not be found in the received document and the document content would not be authenticated. A special paper substrate is used to resist document copying.

Keywords: image security, document security, invisible watermarking, fingerprinting, remote printing, cryptography

1. INTRODUCTION

Three relatively recent events have made the notion of remotely printing verifiably-authentic documents a practical reality. Those events are the development of a secure and trustworthy Internet infrastructure, the means of inexpensively composing, watermarking, circulating and printing digital images, and the "Electronic Signatures in Global and National Commerce Act" which has legally recognized electronic signatures. If the results of these developments are combined with serially numbered fraud resistant paper substrates on which the digital images are printed, this reality extends even to printing high-value documents that can approach the trustworthiness of currency. In these processes there are a number of *conditions of trustworthiness* that must be satisfied to justify these claims. In this paper the conditions will be listed and a solution will be outlined for each of them.

The *conditions of trustworthiness* will be examined in the context of issuing and remotely printing marine insurance certificates by the fictitious **Trusted National Marine Insurance Co.**, which will be referred to herein as the "Originator." Marine insurance certificates are important high-value documents because, when combined with other documents such as the ship's manifest and bill of lading, they become enabling collateral for the issuing of loans secured by the cargo. As will be seen in the example, insured valuation of a ship's cargo routinely can reach tens of millions of dollars.

2. THE INTERNET MODEL FOR REQUESTING A TRUSTWORTHY DOCUMENT

In addition to the Originator, there exists another enabling entity that will be identified as **TrustProcess.com,** or more succinctly herein, as the "Trust-Process.**"** The Trust-Process embodies the required secure and trustworthy connections between the Originator and, in our example, the shipping company, referred to herein as the "Client." Hence, our model system involves three entities - the "Originator," the "Client," and the "Trust Process," the last of which does much to appropriately create and authenticate each document.

The Trust-Process may be operated by the Originator or it may be a separate entity operating as the Originator's agent to enable the connection between the Originator and the Client. When the Client determines that it has an insurable interest, the Originator is contacted using the Trust-Process' Internet interface. *Condition of trustworthiness #1* occurs on this initial contact with verification of the legitimacy of the Client's identity by the Trust-Process. (We will have more to say about each *condition of trustworthiness* subsequently, but let it suffice for now to identify a need for each of them.)

With the Client's identity verified, the Originator's interrogative is presented on the screen of the Client's workstation. The Client enters the identity of the insured party, a description of the cargo and its insurable value, the approximate starting date of transit, the name of the vessel, the ports of departure and arrival, and any other information required by the Originator. This body of information, as a whole, will be referred to herein as the "particulars." The Trust-Process acknowledges receipt of the particulars and passes them along to the Originator, and the Client disconnects from the Trust-Process. *Condition of trustworthiness #2* occurs on the transmission of information between the Client and the Trust-Process and between the Trust-Process and the Originator. These transmissions, which will likely be made over a public network, must not be readable by a third party and they must be essentially impervious to undetectable tampering; in other words, they must be "secure transmissions."

When the Originator receives the Client's identity and the particulars from the Trust-Process, the insurance premium is established, the particulars are augmented with additional information, such as the Client's "Open Policy" number and the relevant insurance form identification, and the Client is billed. The augmented particulars are, as yet, only a few hundred bytes of information, yet they uniquely specify the entire certificate of insurance. The augmented particulars are passed back to the Trust-Process for preparation of the final certificate that will be returned to the Client in the form of a digital image. Note that all transmissions between the Originator and the Trust-Process are secure transmissions, as defined above.

3. THE INTERNET MODEL FOR DELIVERING A TRUSTWORTHY DOCUMENT

In an "all-digital" world, the process of purchasing insurance could be completed by the Trust-Process sending the Client a digital receipt signed with the Originator's electronic signature. But in our traditional paper-based culture, paper certificates are still the norm and will likely remain so well into the future. However, there are now methods that can be used to print a verifiably-authentic certificate of insurance using the Client's ink-jet or laser color printer. The enabling methodology resides wholly within the Trust-Process and it is accomplished using a carefully composed digital image, shown in Figure 4, that is transmitted to the Client for printing by the Client's printer on a serially numbered blank form, shown in Figure 5.

The Client is notified by unsecure e-mail that the certificate is waiting when the Trust-Process is ready to transmit the digital image. The Client again establishes a secure connection to the Trust-Process and, as before, the Client's identity is verified. The Client is then asked to supply the serial number of the next blank form on which the original certificate will be printed. The Trust-Process concatenates the received serial number to the augmented particulars for the certificate, composes a digital image of the certificate, and imbeds a unique invisible watermark into the digital image that is derived from the augmented particulars. In this way the augmented particulars and the invisible watermark are inextricably tied to each other, and that tying is *condition of trustworthiness #3*.

As might be expected, remotely printed verifiably-authentic documents require that a number of additional *conditions of trustworthiness* be satisfied. Because a certificate of insurance can be used as supporting collateral for obtaining a loan, *condition of trustworthiness #4* requires that one, and only one, original certificate be printed by the Client; any other copies must be visibly identifiable as copies. *Condition of trustworthiness #5* requires strong protection against copying of the printed certificate using a color photocopier or by scanning and reprinting. *Condition of trustworthiness #6* requires the

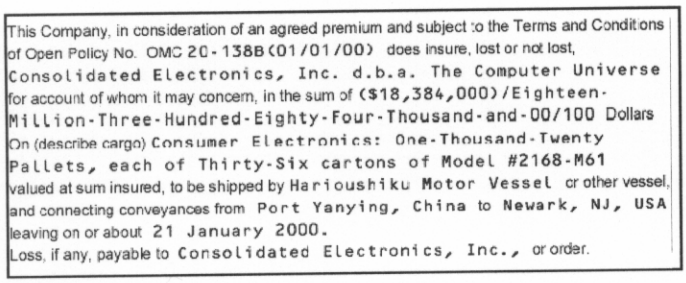

This Company, in consideration of an agreed premium and subject to the Terms and Conditions of Open Policy No. OMC 20-138B(01/01/00) does insure, lost or not lost, Consolidated Electronics, Inc. d.b.a. The Computer Universe for account of whom it may concern, in the sum of ($18,384,000)/Eighteen-Million-Three-Hundred-Eighty-Four-Thousand-and-00/100 Dollars On (describe cargo) Consumer Electronics: One-Thousand-Twenty Pallets, each of Thirty-Six cartons of Model #2168-M61 valued at sum insured, to be shipped by Hariooshiku Motor Vessel or other vessel, and connecting conveyances from Port Yanying, China to Newark, NJ, USA leaving on or about 21 January 2000.
Loss, if any, payable to Consolidated Electronics, Inc., or order.

Figure 1. The "Partially-Augmented Particulars" of the Certificate of Insurance supplied by the Client and augmented by the Originator.

```
OMC20-138B(01/01/00)ConsolidatedElectronicsIncd
baTheComputerUniverse($18384000)/Eighteen-Milli
on-Three-Hundred-Eighty-Four-Thousand-and-00/10
0ConsumerElectronicsOne-Thousand-TwentyPalletse
achPaletofThirty-SixcartonsofModel#2168-M61Hari
oushikuMotorVesselPortYanyingChinaNewarkNJUSA21
January2000ConsolidatedElectronicsInc123456
```

Figure 2. The "Message" excerpted from the "Augmented Particulars" by removing white-space and small punctuation characters. Note the form serial number appended at the end.

HMAC-1, in turn, is based on the Secure Hashing Algorithm (SHA-1),[5] which is widely accepted as an extremely strong one-way hash with excellent collision resistance. SHA-1 is a compression hashing algorithm accepting a message of any finite number of bytes and producing a twenty byte (160 bit) hash. Symbolically, if s_i is the input character string of any finite length and s_o is a byte string twenty bytes in length, the secure hashing function **SHA** produces s_o given s_i, or

$$s_o = \mathbf{SHA}(s_i).$$

The Message Authenticating Code function, **HMAC**, requires two arguments, k, a 64 byte secret key, and m, a message character string of any length, and it produces a twenty byte string, s_m. **HMAC** is based on the function **SHA,** and can be stated concisely as:

$$s_m = \mathbf{HMAC}(k, m) = \mathbf{SHA}(k \wedge p_o \,||\, \mathbf{SHA}(k \wedge p_i \,||\, m)),$$

where the symbols "$a \wedge b$" mean the bit-wise exclusive-or of a with b, the symbols "$a \,||\, b$" mean that b is concatenated to the right end of a, and where p_o is a 64 byte string of the repeated byte $5C_{16}$, where 5 and C are hexadecimal digits from the set [0,...,9,A,...,F], and p_i is a 64 byte string of the repeated byte 36_{16}. Each instanciation of **HMAC** requires two instanciations of **SHA**, as shown.

The invisible robust watermarking method[6] that will be used imbeds values from a pseudo-random watermarking plane into the image of the certificate by modulating the brightness of every pixel of the image. The watermarking plane is generated using a sequence of uniformly distributed random numbers. The **HMAC** function can be used to create just such a sequence, and the sequence so created will have excellent statistical properties. To do this, **HMAC** is used in a recursive form with feedback, as:

$$_nr = \mathbf{HMAC}(k, {}_{(n-1)}r) \,||\, N,$$

where $_nr$ is a sample of twenty bytes produced on the n-th iteration, N is an eight-byte big-endian representation of n, and the initial values $_0r = m$ and $N = n = 1$. Thus, for each iteration, a new sample of twenty bytes having pseudo-random values is produced, and more importantly, the entire sequence is inextricably tied to the secret cryptographic key and the message, which, in turn, is generated form the augmented particulars of the certificate. Therefore, the invisible watermark that is to be permanently imbedded into the image of the certificate using the generated watermarking plane is another, more subtle form of the Message Authentication Code generated from the message and the secret key.

4.4 Condition of Trustworthiness #4: Enforcing a single valid copy

Because the certificate of insurance is one of several documents that can serve as collateral to secure a loan, it is important for fraud deterrence to allow only one valid copy to be printed by the Client. In general, however, the problem of restricting the number of copies that the Client can print is intractable; the Client with little effort can print as many as he wants. Controlling the number of valid copies that can be printed requires control of the Client's ability to print, which the Trust-Process will not have, or control of the paper on which the Client is to print, which the Trust-Process can have. This can be enforced by requiring valid certificates to be printed on serially numbered forms supplied by the Originator, with the format of the form known to the Trust-Process. Any reputable securities printer can supply serially numbered forms and will certify that no two of them have the same number. The reason for requesting the form serial number from the Client before transmitting the image of the certificate now becomes apparent. That serial number can be included as part of the image of the certificate to be printed by the Client. The echoed number could be printed near the preprinted serial number on the form with a caption such

printed certificate to be strongly resistant to fraudulent alteration. And, finally, *condition of trustworthiness #7* requires the physical certificate to be analyzable by automated means to verify the authenticity of its particulars.

4. SATISFYING THE *CONDITIONS OF TRUSTWORTHINESS*

By now, hopefully, the reader has a mental picture of the process of issuing a verifiably-authentic document, providing each of the *conditions of trustworthiness* can be satisfied. Each of *conditions of trustworthiness* will now be discussed individually to add substance to the previous claims.

4.1 Condition of Trustworthiness #1: Verifying the Client's identity

It is important in the example application (and in most others, as well) for the Originator to establish the identity, and thereby the legitimacy, of the Client on every contact. Much of business relies on trusted relationships that are established by an untarnished reputation or by long-term familiarity between known parties. In the impersonal digital-world, identity and legitimacy are established using a digital-certificate issued by a trusted third party. Digital-certificates are issued by companies such as VeriSign [1] or Entrust.[2] They are the electronic equivalent of a letter of introduction from a trusted third party. Although neither company routinely discloses the depth of verification done before a digital certificate is issued, it is believed that the verification is not trivial. The Trust-Process relies on digital certificates for Client identification; other authentication technologies may be used as appropriate.

4.2 Condition of Trustworthiness #2: Secure transmission paths

All transmissions passed between the Client and the Trust-Process and between the Trust-Process and the Originator must be "secure." The transmissions will likely be made over a public network where their contents are viewable at every node through which they pass, and routing paths within the network are generally not predictable or controllable. The only way to make these transmissions "secure" is to make them unreadable by anyone except the intended recipient. This is accomplished using cryptography. Public-key encryption;[3] verification that the public keys of the Client, the Trust-Process and the Originator are, in fact, legitimate; secret key exchanges; and other mechanisms to ensure secure communication paths are imbedded in the Secure Sockets Layer (SSL) of most Internet browsers, and will be employed by the example application.

4.3 Condition of Trustworthiness #3: Inextricable tying of the particulars to the invisible image watermark

The Client's response to the Originator's interrogative produces a group of character strings that identify the insured party, the cargo, its insurable value, etc., which collectively are called the particulars. The Originator may augment this list with some additional character strings, such as the Client's "Open Policy" identifier and the form number and its revision level on which the certificate of insurance is to be printed. The augmented list uniquely specifies the certificate of insurance. One further addition is made to the augmented particulars and it is the serial number of the blank form on which the certificate will be printed by the Client. The reason for inclusion of the particular serial number will be discussed shortly. Figure 1 illustrates the certificate particulars. The augmented particulars must be inextricably tied to an invisible watermark placed in the resulting image of the certificate if it is to become verifiably authentic. The particulars or augmented particulars may be stored by the Originator or the Trust-Process or, for business models where information privacy is required, may be discarded after the transaction is complete. As it will be shown below, the document's watermark and its textual contents are sufficient for authentication and no permanent storage of the particulars is required.

To begin the process of watermark creation, all of the character strings of the augmented particulars are concatenated to form a single longer character string, and the small punctuation marks (periods, commas, colons and semicolons) and "white-space" characters (blanks, tabs, new-line) are removed from the longer string, which will be called the "message." Figure 2. illustrates the message condensed from the particulars in Figure 1. (Note, the terms "byte" and "character" are used interchangeably herein, both referring to an entity having eight binary bits. The only difference is that a character has an associated printable symbol.) The message is then processed to form an extremely secure Message Authentication Code (MAC). Creation of a MAC from the message requires a secret cryptographic key known only to the Trust-Process. The particular MAC generating process used is known as HMAC-1,[4] which has been carefully analyzed and constructed to minimize the probability of secret key exposure and to minimize the ability to predict an alteration of the message that would produce the same MAC. The resulting MAC is 160 bits in length.

as "VOID IF BOTH CERTIFICATE NUMBERS ARE NOT THE SAME," as shown in Figure 3. As an additional security measure against fraudulent alterations, the serial number requested from the Client is also included as part of the augmented particulars for the certificate. It is, therefore, inextricably tied to the MAC and the image watermarking plane derived from the MAC. Shortly we will see that the serial number also participates in the authentication process.

4.5 Condition of Trustworthiness #5: Protection against duplication by photocopier

For the same reasons given in subsection 4.4, it is important to have strong measures against duplication of valid certificates by photocopier. Since the document is printed remotely on the Client's printer, there can be no "handwritten countersignature with blue ball-point pen" that can be verified on the valid certificate but not on the copy. The imbedding of copier-resistant artifacts in printable digital images is an interesting research problem, but the authors know of no successful general solution to the problem. But some securities printers have demonstrated significant copy resistant features in their paper substrates. Collaboration with one, VerifyFirst Technologies,[7] has demonstrated that many of their copy-resistant and antifraud features are or can be made to be compatible and non interfering with the invisible robust watermarking method used. Some of VerifyFirst's antifraud features that have been tested for compatibility are TAMPERSAFE®, which are lenticular holograms having several engraved latent images; TOUCHSAFE™, which allows instant interactive verification of an original certificate by touch; THERMOSAFE™, which causes the word "VOID," "COPY," or "ALERT" to appear when photocopied; NONDUPIT™ which causes a phantom seal or signature block to disappear when photocopied; METALLICSAFE™, which is a metallic foil serial number on variegated background that does not photocopy, and others. It is shown in Figure 3 that even with special lighting conditions only a faint image of the metallic foil certificate number is visible in a scanned copy, but the echoed serial number contained in the digital image and printed below it is obvious. Under photocopier lighting, the metallic foil serial number becomes indistinguishable from its variegated background. The metallic foil in METALLICSAFE™ has also been tested recently and found compatible with an IBM color laser printer. Using some or all of these antifraud features in the Originator supplied forms can create a printed certificate that strongly resists photocopying.

Figure 3. A faint METALLICSAFE™ serial number with an echoed "self-voiding" serial number printed below.

4.6 Condition of Trustworthiness #6: Protection against fraudulent alterations

Remotely printed certificates must be strongly resistant to fraudulent alterations. A document that is in the form of a digital image can be altered relatively easily using an image editor. The particulars are vulnerable since they are text strings. The image is protected by encryption against alteration during transmission, but once received and decrypted, fraudulent alterations are possible. The MAC, and the invisible watermark derived form the MAC, have been included to protect against such alterations. The MAC, generated using a secret cryptographic key[8] that would be unknown to anyone attempting to defraud, permits detection of any change in the message with a probability approaching certainty. As an example, the original MAC produced by the message in Figure 2. is:

$$\text{FE 9C 6E C4 2A 72 F7 EE 80 A9 F6 A7 BD 7E B8 70 F7 B4 C8 C3}_{16}.$$

Alteration of a single bit in the message, for example, changing the first character "2" to a "3" produces an altered MAC that is:

$$\text{67 D3 2C 21 8E 71 93 74 38 16 81 6B 50 42 D0 28 B6 A5 8B B8}_{16},$$

and the watermarking plane derived from the altered MAC is radically different from the one derived from the original MAC. Thus, verifying that a watermark in the image can be derived from the augmented particulars in the image by knowing only the secret cryptographic key gives indication approaching certainty that the augmented particulars have not been altered. This, by design, includes the preprinted serial number of the paper on which the certificate is printed, since it is included in the augmented particulars.

4.7 Condition of Trustworthiness #7: Authentication of the printed certificate

Authentication is accomplished from a scan of the physical certificate that approximately recreates the digital image. The scan can be done at a remote site, at a bank, for instance, where the certificate may have been taken to be used as loan collateral. The digital color image produced by the scanner is compressed and transmitted to the Trust-Process for authentication, again using a secure connection and with establishment of the legitimacy of the bank and the Trust-Process.

On receiving the digital image, the Trust-Process peels out the particulars using Optical Character Recognition (OCR) methods. From the recognized particulars, the document record can be located in the archives of the Trust-Process and the secret cryptographic key used in forming the MAC can be recalled. A candidate message is reconstructed from the recognized particulars, and from it, a candidate MAC is produced using the recalled secret key. A watermarking plane is derived and reconstructed using the candidate MAC. The received image is automatically realigned and resized[9] to the size of the original and watermark detection is attempted using the reconstructed watermarking plane. If the reconstructed watermark is detected in the realigned scanned image, then the authenticity of certificate particulars is established with a probability that approaches certainty. The sender of the digital image would be notified that the document particulars are likely authentic and would be reminded to visually check a list of physical security features that should be in the paper substrate on which the certificate was printed. This will include special emphasis on checking and matching the two certificate serial numbers, the one echoed originally in the digital image created by the Trust-Process and the one preprinted on the paper substrate.

The quality required of the scanned image is not demanding. Inexpensive flatbed scanners scanning at 200 to 300 pixels/inch produce a facsimile image of more than sufficient quality for watermark detection with the watermarking method used. To decrease the demands on OCR, a more easily recognized OCR font is used in the original digital image of the certificate sent from the Trust-Process, and the text of the particulars is printed on small uninked (and unwatermarked) fields of the substrate. To facilitate alignment of the scanned image with the original, realignment aids are also included in the original digital image.

In some applications the MAC can be included as printable hexadecimal characters in the original digital image instead of the watermark. The weakness of this method in the presence of document duplication is obvious. An automated authentication program can be spoofed to authenticate the particulars and MAC that were printed on a blank sheet of paper. However, it is worth noting that there are a number of applications where the existence of duplicate documents may be of little consequence (for example, a mortgage commitment or a death certificate), but the verifiable authenticity of their particulars is of considerable importance.

5. CONCLUSIONS

A complete Internet-based system for the remote production of verifiably-authentic and duplication-resistant documents has been presented. Although presented in the context of printing high-value marine insurance certificates, the concept can be extended easily to other document types. These might include contracts, medical prescriptions, public records, receipts, coupons, … even college transcripts. Each type can place different constraints on the Trust-Process. For example, all types imply secure cryptographic key management, but the expected life of a marine insurance certificate may be only a few months, the expected life of a medical prescription a few years, but the expected life of a birth certificate will be more than one hundred years. Long term storage of digital records is increasingly important on its own, and the rapid obsolescence of digital storage technologies is just one of its issues. The strength of security features needed for a $10,000 life insurance policy is likely to be less than that for a $18,000,000 marine insurance certificate. Various state and federal statutory constraints also exist that may prohibit the application of such technology unless and until they are updated to be more in compliance with the Federal Electronic Signatures Act.

It is important to reemphasize that the Trust-Process does not require storage of identifiable personal data. This is very important, as stated above, for applications where personal privacy is an ethical and legal requirement. If, for example, the application produces electronic prescriptions, a patient's identity would exists only transiently in the Trust-Process and would

never be retained. Only the secret cryptographic key used for constructing the MAC and the derivative watermarking plane needs to be securely kept for prescription authentication. An unencrypted pointer to that specific key can be placed on the printed prescription form to be read at the time of authentication. All other information needed for authentication resides in the image watermark (or in a printed MAC) and in the reconstructed "message" recognized by OCR from the scan of the printed prescription.

The Internet-based system described has a reasonable and straightforward migration path to an eventual "all-digital" embodiment where completed transactions are acknowledged by sending an electronic receipt to the Client that has been signed with the electronic signature of the Originator.

5. REFERENCES

1. VeriSign, Inc., Mountain View, CA. VeriSign is a provider of Internet trust services including authentication, validation, payment and managed PKI.
2. Entrust Technologies, Inc., Plano, TX. Entrust is a provider of Internet security services, including Public-key Infrastructures (PKI) and digital certificates.
3. A. Menezes, P. van Oorschot, & S. Vanstone, **Handbook of Applied Cryptography**, CRC Press, New York, NY, 1997, pp. 283-319.
4. M. Bellare, R. Canetti, and H. Krawczyk, "Keyed Hash Functions and Message Authentication", Proceedings of Crypto'96, LNCS 1109, pp. 1-15.
5. A. Menezes, et al., above cit., pp. 348-349; also ANSI X9.30-2.
6. G. Braudaway, "Protecting Publicly-Available Images with an Invisible Image Watermark," IEEE International Conference on Image Processing, (ICIP'97), Santa Barbara, CA, October 26-29, 1997, pp. 524-527.
7. VerifyFirst Technologies, Paso Robles, CA. VerifyFirst provides security printing utilizing security inks, thermochromic inks, void pantographs and other security technologies. TAMPERSAFE®, TOUCHSAFE™, THERMOSAFE™, NONDUPIT™ and METALLICSAFE™ are trademarks of VerifyFirst Technologies.
8. The secret cryptographic key used to produce the original and altered HMAC is the 48 character string "The violins of spring sing sweetly in the breeze". By the rules of HMAC, it is right-padded with sixteen bytes of 00_{16} to a 64-byte length. If the key had been longer than 64 bytes, it first would have been reduces to 20 bytes with a single instanciation of the **SHA** algorithm and then right-padded with 44 bytes of 00_{16}.
9. G. Braudaway & F. Mintzer, "Automatic Recovery of Invisible Image Watermarks from Geometrically Distorted Images," **Journal of Electronic Imaging**, Vol. 9, No. 4, October 2000, pp. 477-483.

(PLACE AND DATE)

CERTIFICATE NO. 123456

VOID IF BOTH CERTIFICATE NUMBERS ARE NOT THE SAME.

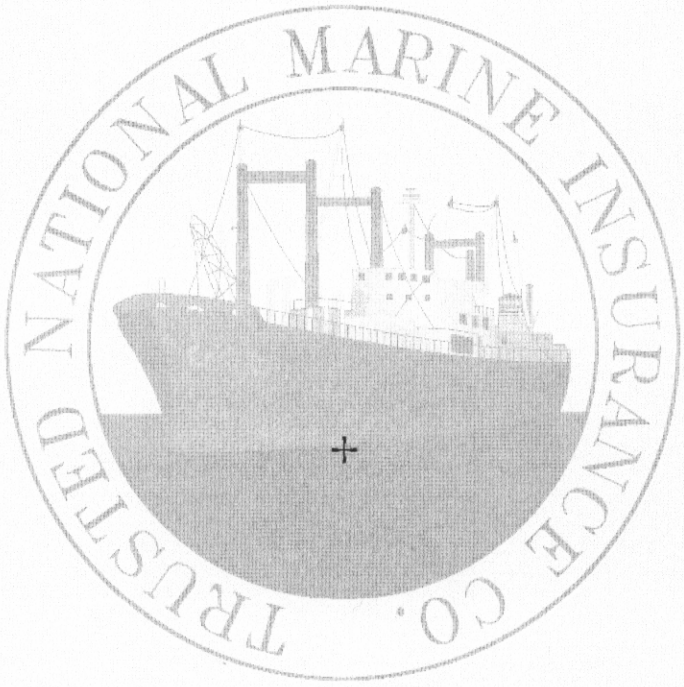
MARKS AND NUMBERS

This Company, in consideration of an agreed premium and subject to the Terms and Conditions of Open Policy No. OMC 20-138B(01/01/00) does insure, lost or not lost, Consolidated Electronics, Inc. d.b.a. The Computer Universe for account of whom it may concern, in the sum of ($18,384,000)/Eighteen-Million-Three-Hundred-Eighty-Four-Thousand-and-00/100 Dollars On (describe cargo) Consumer Electronics: One-Thousand-Twenty Pallets, each of Thirty-Six cartons of Model #2168-M61 valued at sum insured, to be shipped by Harioushiku Motor Vessel or other vessel, and connecting conveyances from Port Yanying, China to Newark, NJ, USA leaving on or about 21 January 2000.

Loss, if any, payable to Consolidated Electronics, Inc., or order.

This insurance is subject to the following current American Institute Clauses of the above certificate:

F.C. & S. and S.R. & C.C. Warranties: Nuclear Exclusion Warranty. Marine Extension Clauses. 60 Day South American Clause. Deliberate Damage-Pollution Hazard Clause. S.R. & C.C. Endorsement and war Risk Insurance.



SPECIAL CONDITIONS

Goods and **merchandise,** except while on the deck of an ocean vessel shipped under an **On-Deck Bill of Lading** are insured:

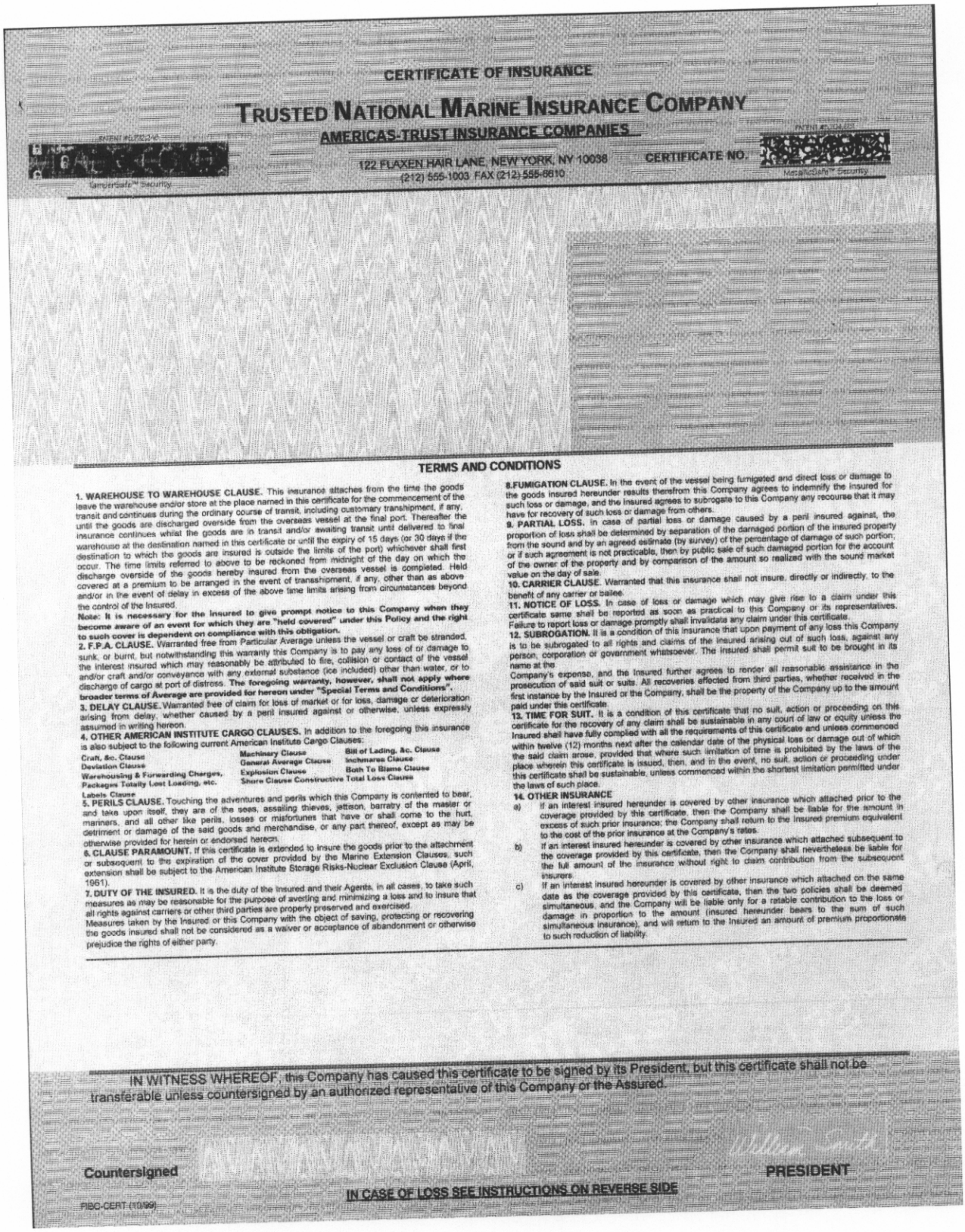
To cover against all risks of physical loss or damage from any external cause, irrespective of percentage, but excluding, nevertheless, the risks of war, strikes, riots,seizure, detention and other risks, excluded by the F.C. & S. (Free of Capture & Seizure) Warranty and the S.R. & C.C. (Strikes, Riots and Civil Commotions) Warranty in this Certificate, excepting to the extent that such risks are specifically covered hereon.

Goods and **merchandise** while on the deck, under an **On-Deck Bill of Lading** are insured:

Free of particular average unless the vessel being stranded, sunk, burnt, on fire, or in collision but including jettison and/or washing overboard irrespective of percentage.

For authentication, contact http://www.TrustProcess.com

Figure 4. The digital image ready to be transmitted to and printed by the Client on the paper substrate shown in Figure 5. The printed image on substrate form a verifiably-authentic "Certificate of Insurance." On white paper, as shown here, the subliminally invisible image watermark is the very faint background texture pattern.



CERTIFICATE OF INSURANCE

TRUSTED NATIONAL MARINE INSURANCE COMPANY

AMERICAS-TRUST INSURANCE COMPANIES

122 FLAXEN HAIR LANE, NEW YORK, NY 10038
(212) 555-1003 FAX (212) 555-8810

CERTIFICATE NO.

TERMS AND CONDITIONS

1. WAREHOUSE TO WAREHOUSE CLAUSE. This insurance attaches from the time the goods leave the warehouse and/or store at the place named in this certificate for the commencement of the transit and continues during the ordinary course of transit, including customary transhipment, if any, until the goods are discharged overside from the overseas vessel at the final port. Thereafter the insurance continues whilst the goods are in transit and/or awaiting transit until delivered to final warehouse at the destination named in this certificate or until the expiry of 15 days (or 30 days if the destination to which the goods are insured is outside the limits of the port) whichever shall first occur. The time limits referred to above to be reckoned from midnight of the day on which the discharge overside of the goods hereby insured from the overseas vessel is completed. Held covered at a premium to be arranged in the event of transshipment, if any, other than as above and/or in the event of delay in excess of the above time limits arising from circumstances beyond the control of the Insured.
Note: It is necessary for the Insured to give prompt notice to this Company when they become aware of an event for which they are "held covered" under this Policy and the right to such cover is dependent on compliance with this obligation.

2. F.P.A. CLAUSE. Warranted free from Particular Average unless the vessel or craft be stranded, sunk, or burnt, but notwithstanding this warranty this Company is to pay any loss of or damage to the interest insured which may reasonably be attributed to fire, collision or contact of the vessel and/or craft and/or conveyance with any external substance (ice included) other than water, or to discharge of cargo at port of distress. **The foregoing warranty, however, shall not apply where broader terms of Average are provided for hereon under "Special Terms and Conditions".**

3. DELAY CLAUSE. Warranted free of claim for loss of market or for loss, damage or deterioration arising from delay, whether caused by a peril insured against or otherwise, unless expressly assumed in writing hereon.

4. OTHER AMERICAN INSTITUTE CARGO CLAUSES. In addition to the foregoing this insurance is also subject to the following current American Institute Cargo Clauses:

Craft, &c. Clause	Machinery Clause	Bill of Lading, &c. Clause
Deviation Clause	General Average Clause	Inchmaree Clause
Warehousing & Forwarding Charges,	Explosion Clause	Both To Blame Clause
Packages Totally Lost Loading, etc.	Shore Clause Constructive Total Loss Clause	
Labels Clause		

5. PERILS CLAUSE. Touching the adventures and perils which this Company is contented to bear, and take upon itself, they are of the seas, assailing thieves, jettison, barratry of the master or mariners, and all other like perils, losses or misfortunes that have or shall come to the hurt, detriment or damage of the said goods and merchandise, or any part thereof, except as may be otherwise provided for herein or endorsed hereon.

6. CLAUSE PARAMOUNT. If this certificate is extended to insure the goods prior to the attachment or subsequent to the expiration of the cover provided by the Marine Extension Clauses, such extension shall be subject to the American Institute Storage Risks-Nuclear Exclusion Clause (April, 1961).

7. DUTY OF THE INSURED. It is the duty of the Insured and their Agents, in all cases, to take such measures as may be reasonable for the purpose of averting and minimizing a loss and to insure that all rights against carriers or other third parties are properly preserved and exercised. Measures taken by the Insured or this Company with the object of saving, protecting or recovering the goods insured shall not be considered as a waiver or acceptance of abandonment or otherwise prejudice the rights of either party.

8. FUMIGATION CLAUSE. In the event of the vessel being fumigated and direct loss or damage to the goods insured hereunder results therefrom this Company agrees to indemnify the Insured for such loss or damage, and the Insured agrees to subrogate to this Company any recourse that it may have for recovery of such loss or damage from others.

9. PARTIAL LOSS. In case of partial loss or damage caused by a peril insured against, the proportion of loss shall be determined by separation of the damaged portion of the insured property from the sound and by an agreed estimate (by survey) of the percentage of damage of such portion; or if such agreement is not practicable, then by public sale of such damaged portion for the account of the owner of the property and by comparison of the amount so realized with the sound market value on the day of sale.

10. CARRIER CLAUSE. Warranted that this insurance shall not insure, directly or indirectly, to the benefit of any carrier or bailee.

11. NOTICE OF LOSS. In case of loss or damage which may give rise to a claim under this certificate same shall be reported as soon as practical to this Company or its representatives. Failure to report loss or damage promptly shall invalidate any claim under this certificate.

12. SUBROGATION. It is a condition of this insurance that upon payment of any loss this Company is to be subrogated to all rights and claims of the insured arising out of such loss, against any person, corporation or government whatsoever. The Insured shall permit suit to be brought in its name at the Company's expense, and the Insured further agrees to render all reasonable assistance in the prosecution of said suit or suits. All recoveries effected from third parties, whether received in the first instance by the Insured or the Company, shall be the property of the Company up to the amount paid under this certificate.

13. TIME FOR SUIT. It is a condition of this certificate that no suit, action or proceeding on this certificate for the recovery of any claim shall be sustainable in any court of law or equity unless the Insured shall have fully complied with all the requirements of this certificate and unless commenced within twelve (12) months next after the calendar date of the physical loss or damage out of which the said claim arose, provided that where such limitation of time is prohibited by the laws of the place wherein this certificate is issued, then, and in the event, no suit, action or proceeding under this certificate shall be sustainable, unless commenced within the shortest limitation permitted under the laws of such place.

14. OTHER INSURANCE

a) If an interest insured hereunder is covered by other insurance which attached prior to the coverage provided by this certificate, then the Company shall be liable for the amount in excess of such prior insurance; the Company shall return to the Insured premium equivalent to the cost of the prior insurance at the Company's rates.

b) If an interest insured hereunder is covered by other insurance which attached subsequent to the coverage provided by this certificate, then the Company shall nevertheless be liable for the full amount of the insurance without right to claim contribution from the subsequent insurers.

c) If an interest insured hereunder is covered by other insurance which attached on the same date as the coverage provided by this certificate, then the two policies shall be deemed simultaneous, and the Company will be liable only for a ratable contribution to the loss or damage in proportion to the amount insured hereunder bears to the sum of such simultaneous insurance), and will return to the Insured an amount of premium proportionate to such reduction of liability.

IN WITNESS WHEREOF, this Company has caused this certificate to be signed by its President, but this certificate shall not be transferable unless countersigned by an authorized representative of this Company or the Assured.

Countersigned

PRESIDENT

IN CASE OF LOSS SEE INSTRUCTIONS ON REVERSE SIDE

FIBC-CERT-(10/99)

Figure 5. A pre-numbered paper substrate, manufactured by VerifyFirst Technologies and containing numerous security features, on which the digital image in Figure 4 is printed to create a "Certificate of Insurance."