DIGIMARC®

INTRODUCTION

This white paper provides a response to a NIST request from the October 7, 2004 meeting regarding the Homeland Security Presidential Directive/Hspd-12 and the Personal Identity Verification (PIV) system. The paper discusses threats to ID security and demonstrates the need to link a physical document, on-card chip data and on-card chip. In addition, the paper describes digital watermarking (DWM) as a valuable technology that can interlink these elements, as well as provide identity source document verification thus establishing and preserving a "chain of trust" for an issued ID credential.

More specifically, this white paper includes:

- An overview of new challenges facing identity verification
- A proposed method of standardizing the linking of a physical card, digital photo and chip
- The critical role of digital watermarking as a necessary security layer
- An overview of digital watermarking technology
- An analysis of NIST's critical threats inherent in PIV applications with proposed countermeasures to these threats using digital watermarking
- A proposed secure ID system architecture using digital watermarking to verify identity source documents and establish a "chain of trust"
- Conclusion with suggestions for the new NIST FIPS-201 standard

NEW CHALLENGES OVERVIEW

The threat of digital counterfeiting and forgery of ID cards is growing at an increasing rate. The ease of digital imaging and pervasiveness of low-cost, easy-to-use PC editing and printing tools have not only made counterfeiting and forgery easier for professional organizations, such as terrorist groups; it has also made this form of counterfeiting a crime of opportunity that is within the capabilities of the average citizen. While document security features continue to improve, and new digital production means offer improved defenses, attacks by both professional organizations and casual counterfeiters are growing threats that pose great and escalating national and geo-political security risks.

DIGIMARC®

Industry Trends

As technology advances and the need increases for greater data-carrying capacity on ID cards, there is a move to adopt chip-based ID cards for various federal programs. While incorporation of a chip can add additional data capacity to an ID card, and digital encryption methods can bolster protection against data alteration or bearer substitution, it is important to note that some counterfeiting and alteration threats remain.

Common Identity Card Counterfeit and Forgery Techniques

The most common attacks on the identity card fall into three general categories: data/photo substitution and alteration, wholesale counterfeit card production, and the compromise of chip security features. All of these attacks focus on the card itself, whereas the secure ID system architecture described later in this paper encompasses a complete secure ID system.

DATA / PHOTO SUBSTITUTION AND ALTERATION

While chips employ sophisticated security algorithms to ensure secure data access and integrity, these technologies are by no means tamper proof. While it may be beyond the capabilities of a casual forger to compromise the chip's security model, there are examples where sophisticated criminal organizations have successfully altered the data contained in a chip. Furthermore, information and components from several valid cards can be combined to create false ID documents.

COUNTERFEIT CARDS

Another very real concern for issuing authorities and inspection personnel is that a criminal can easily obtain a blank card complete with a chip. This card, personalized on a typical card printer, can easily appear to be genuine, complete with readable data contained on the chip. This blank card may also be combined with elements of a valid (possibly stolen) issued card.

COMPROMISING THE CHIP OR READER

Another attack is to "break" the chip on the card, or disable the card chip reader. Because chips are active security components and, as such, have a real failure rate, intentionally disabling a card or reader can be interpreted by an authority as a card or reader malfunction, thereby allowing authorization of an invalid card holder. For example, if a small percentage of cards fail to successfully read, particularly in lower security entry points, the inspectors may allow some people through security who present ID cards that don't read, simply predicated upon visual confirmation of the card and a few simple

questions. In reality the physical card may have been forged and the chip purposely disabled or the reader jammed to bypass standard security procedures.

LINKING THE PHYSICAL CARD, DIGITAL PHOTO AND CHIP

Multiple security layers can be used to thwart the previously discussed substitution/alteration and counterfeit attack classes. One security layer can be used to verify that the digital information on the chip has not been altered. Another security layer can be used to uniquely link the digital photo file on a chip to a particular physical chip data carrier component. A further security layer can be used to link a printed photo (as well as printed demographics) on a physical card to the chip data carrier component contained on the card. The current draft NIST standard addresses the first security layer, but does not address the latter two security layers.

A security layer linking the printed photograph and demographic data to the physical card provides resistance to the attack of compromising the chip or reader. The current draft NIST standard does not address this security layer.

Thus, the interlinking of the printed photo, digital photo and chip is not only part of a layered security system, but is also a critical layer of security.

As such, Digimarc recommends incorporating a standard electronically readable code that interlinks the printed photo, digital photo on the chip, and chip card serial number in a fixed field format of 96 bits. Furthermore, Digimarc recommends combining information describing the printed photo, a summary of bearer demographic information (e.g. initials), and a unique card number identifying the physical card as elements of the same electronically readable 96 bit code structure. The demographic data and card number may also be printed in human readable form and/or included in the bar code or magnetic stripe.

DIGITAL WATERMARKING AS A SECURITY LAYER

As mentioned, the proliferation of inexpensive and ubiquitous digital technology has facilitated digital counterfeiting over the last few years. However, it can also be used to stem the tide. A number of technologies have been developed to help ensure the integrity of officially issued identity documents and to protect against counterfeiting and

forgery. Key among these is digital watermarking, which creates a highly effective, covert digital security layer.

The security attacks already discussed can be mitigated by the incorporation of a digital watermarking security feature which, when used in combination with chip-based security features, creates an effective machine-readable secure ID document. Digital watermarking is a covert digital security feature that can be used to fuse multiple elements of identity documents into a coherent secure ID structure, incorporating both the text, graphics and photographic information printed on the card with digital data, including facial image, stored on the chip. This layered, interlocking approach enhances the overall integrity and security of a documents.

Digital watermarking is a proven technology that is deployed as a covert, machine-readable security feature in driver licenses in the U.S. and in Europe; is used successfully by major entertainment companies and stock photography firms to communicate copyrights; and supports global counterfeit currency deterrence programs through Digimarc's work with a consortium of international central banks.

ENHANCING PERSONAL IDENTITY VERIFICATION WITH DIGITAL WATERMARKS

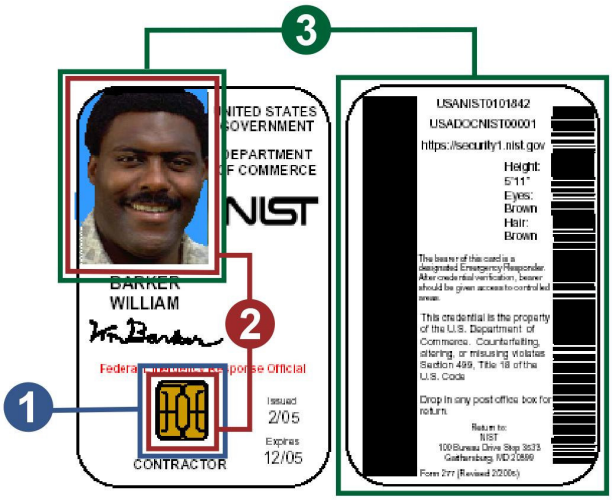
DIGIMARC®

DIGITAL WATERMARKING ENABLED DIGITAL SECURITY LAYERS

1 Interlock digital image and chip.
Embedding the serial number of the chip (or other unique identifier) in the image stored on the chip ensures no image modification has taken place and the chip is original and not a substitute.

2 Interlock chip and photo.
Embedding the serial number of the chip (or other unique identifier) in the printed image effectively links the chip to the document data while enabling detection of photo substitution.

3 Interlock photo and physical card
Embedding critical data from the physical card in the printed image enables detection of photo substitution and data alteration.



Absence of digital watermark indicates document tampering or simulation.

DIGITAL WATERMARKING TECHNOLOGY OVERVIEW

The digital watermarking security layer is created by embedding covert, machine-readable digital data into the personalized passive image elements of identity documents, such as the printed and/or the digital photo plus background artwork. Using the digital watermarking process, digitally printed elements are first covertly digitally marked and identified as interlocking security elements and are then fused together to protect against data/photo substitution, alteration and counterfeiting. This is a highly effective method to link the chip, and its data, to the physical card using personalized data printed on the face of the card. The embedded digital watermark data is imperceptible to humans, but can be read by computers or other devices equipped with special secure software coupled with a readily available scanning device.

 9405 SW Gemini Drive, Beaverton, OR 97008 T +1.503.469.4800 F +1.503.469.4795 www.digimarc.com

The digital watermarking security layer contains personalized/unique digital identifiers, such as the serial number of the in-card chip, unique identity document number, issuing operator and issuing printer. The embedded data is based on the issuing authority's need to ensure the integrity of the card and easy and reliable verification and forensic analysis of the card. Access to this data is controlled through secure reader software under the control of an authorized issuing authority. Each and every time the facial image is read from the chip, it is possible, in a fraction of a second, to decode and verify this data embedded in the image. At the same time, if a counterfeit card is presented, even if it has readable data in the chip, the absence of the digital watermark in the image read from the chip immediately identifies the counterfeit.

Unlike overt physical data carriers and security features, with digital watermarks there are no obvious security features present to serve as a target for forgery, alteration or duplication. Even if a forger is aware of the existence of a digital watermark, it is virtually impossible to successfully compromise the security feature due to the complexity of the embedding protocol, and the fact that each particular embedded image is variable, unique and image dependant.

Algorithm Details and Secret Keys

Digital watermarking uses proven spread-spectrum techniques to hide the digital data within the luminance of printed images. The embedding process begins with the digital payload to be embedded into an image, uses error correction and error detection techniques to condition the payload to be more robust and reliable, and then modulates a spread-spectrum pseudo-random noise sequence (PNS) with the payload. Once this secured sequence of bits has been generated, it is added to the original image through the use of an efficient, non-linear, human visual system model to increase the covert nature of the signal, resulting in a digitally watermarked image.

The detection process begins by improving the signal-to-noise ratio (SNR) of the embedded data in the digitally watermarked image by blindly separating the embedded data from the image as much as possible. The process then calculates the scale, rotation and offset of the improved SNR image via features of the digital watermark. Once synchronized with the covert digital data, the image is sampled to collect the PNS that was embedded. From the recovered PNS, the digital payload is decoded and any errors are detected and/or corrected. The detection process does not require the original image, known as blind detection.

The spread-spectrum pseudo-random noise sequence (PNS) uses a secret key-driven generator to derive its unique long carrier signals. These keys vary by issuer, document, and often within these domains, and the reader employs a secure key management system to provide authorized access without requiring network connectivity for each read. The PNS also enables digital watermarks to be layered, robust to transformations such as printing, and resistant to a variety of attacks. The error correction, error detection, and perceptual model algorithms increase security when they are kept secret.

In addition, copy attack countermeasures are often included in the digital watermark to thwart removal from one image and impression on a second image, further securing the digital watermark.

Furthermore, the payload can include a digital signature or be encrypted. Due to the size of a digital watermark payload, symmetric key encryption is more applicable than asymmetric or public key methods. However, if the system uses high resolution scanners, larger digital watermark payloads can be incorporated. Additionally, a card can be designed so that multiple payloads can be embedded in multiple elements. For example, one payload can be embedded into the ID photo with one or more additional digital watermarks embedded into background images, thus increasing the overall payload size as well as protecting against highly targeted attacks focusing upon a single element.

Compatibility with Existing and Emerging Technologies

The digital watermark security feature provides a unique level of compatibility with existing and emerging security features, including barcode and magnetic stripe data carriers, and a variety of biometrics. When used in conjunction with these security features, digital watermarking adds an unprecedented layer of digital security that enables positive document verification and forensic analysis and defense in depth.

Independent testing has shown that digital facial images that are secured with the digital watermarking feature are fully compatible with facial recognition algorithms, systems and processes. Additionally, a digital watermark security feature provides the issuing authority flexibility in terms of the issuance environment by offering compatibility with multiple printing methods, including: D2T2, inkjet, digital press, laser printing and laser engraving. This digital security feature can be deployed in a variety of government-

issued identity documents including federal employee IDs, transportation worker IDs, passports, driving licenses, military IDs, voter registration IDs and many more.

Inspection of Digital Watermark Security Feature in Federal Government Employee IDs

An ID card secured with digital watermarking, such as a federal government employee identity card, driver license or other ID, can be easily inspected at a variety of locations by inspection authorities. If the inspection point is equipped with a suitable card reader and secure digital watermarking reader software, the digital watermark feature can be used to automatically verify the card with virtually no impact on the time to complete the inspection process. When the digital watermarking feature is required to be read from a printed image, an appropriate optical scanner device is required. However, in the case of a digital watermark embedded in a facial image stored digitally and electronically on a chip, this reading and decoding of the digital watermark can be done simultaneously with reading the chip data at the point of inspection.

A digital watermarking security feature creates a low cost, yet highly effective interlocking digital security layer that complements and further enhances the security of chip-based ID cards against digital counterfeiting threats. The feature can be reliably inspected using secure software and suitable reading devices to establish the authenticity and integrity of these documents across jurisdictions.

THREATS AND COUNTERMEASURE ANALYSIS

The goal of security features in a personal identity verification system is to greatly raise the cost, time and risk required for a successful attack. Importantly, an issuer can decrease the validity period of a credential to decrease this risk of attack and, in this context, technologies that increase the time required for a successful attack become even more effective for the overall security of a credentialing system.

In general, digital watermarks increase cost and time required for a successful attack by casual and professional counterfeiters, including terrorists, because successful attack upon a digital watermark requires different skills than breaking cryptography, traditional printed security, and electronic chips. Generating and cracking digital watermarks requires sophisticated knowledge of a variety of disciplines including but not limited to: digital signal processing, communication theory and human perceptual modeling. More specifically, in the case of an ID card, a successful attack requires

computing the secret PNS as well as the error correction, error detection, copy attack countermeasures, mapping functions, and non-linear perceptual model algorithms so that the target digital watermark can be created or modified. If the payload is encrypted, the counterfeiter must also attack the encryption of the payload. Because the presence of a digital watermark within an ID card is known only to authorized personnel and must be read by the reader for the card to be verified, attacking the content in an attempt to remove the digital watermark does not lead to a successful attack.

In addition, digital watermarking is a perceptually covert security technology. The fact that it is neither visible nor its presence known, makes it less likely to be attacked.

A secure and private reader greatly increases security since the counterfeiter cannot know whether he has successfully attacked the security features. To this end, the counterfeiter is more likely to be caught when attempting to pass a counterfeit card.

Furthermore, a digital watermark provides local authentication and integrity checking. It does not require connection to a server, and is therefore not susceptible to a communications hack. More specifically, the data embedded in a digital watermark payload is compared to that contained on the card's chip data carrier and/or the physical card itself for verification. This local and contained confirmation aspect is also compatible with privacy concerns.

Finally, digital watermarks can include forensics data, which could identify the issuing operator and printer. This forensic data can be read from confiscated fake ID cards and help in uncovering leaks, thus increasing the risk of counterfeiting. The forensic data can be read offline with human interaction to greatly increase the difficulty of attack.

Digital watermarks are an effective and economically viable security feature that can be used to protect identity documents against attack and compromise by both casual and well funded professional/terrorist organizations.

DIGIMARC®

NIST Threats and Countermeasures, and Digital Watermarking

In terms of the specific threats and countermeasures identified by NIST, Digimarc shows a few additional countermeasures provided by digital watermarking (highlighted below).

Threat	Countermeasure
Cardholder makes improper use of a valid card	✓ Review the use and acceptance of the source documents ✓ Application for identification card made only by the accredited sponsor ✓ Formal review and approval of the application ✓ Inclusion of source document copies with application ✓ Display of source documentation to issuer by "holder" at time of issuance ✓ Verify source documents via a digital watermark during the scanning and saving process
Counterfeiting	✓ Holographic organizational seal of issuer and / or other issuer ID hologram integrated into card ✓ ID or Serial number digitally signed by manufacturer and burned into chip ✓ Digital signature by issuer of all stored identifying information ✓ Encryption of stored identifying information ✓ Mechanism for checking holder ID and card ID or serial number with issuer records ✓ Integration of PIN (not recorded on card) with cryptographic authentication process ✓ Verify via a digital watermark that the physical card or chip data has not been modified
Stolen or borrowed cards are used to gain access	✓ Card accountability procedures (e.g., reporting / publication of lost card lists) ✓ Use of PIN(s) not recorded on card (e.g., in challenge/ response to counter use of lost cards) ✓ Use of biometric input from cardholder and verification at time of access request ✓ Visual inspection of cardholder image with image of person claiming to have been issued the PIV card.

Lower sensitivity cards are used to gain access to more sensitive and critical assets	✓ Different certificates / digital signatures for each level authorized ✓ Color coding or pattern changes on physical card representing level(s) authorized ✓ Local access authorization procedures ✓ Verify the physical card via digital watermarking, even when the chip is broken or a reader is not available

SECURE ID SYSTEM ARCHITECTURE AND DIGITAL WATERMARKING

The security of personal identification verification requires a system approach. This paper has shown how digital watermarking helps secure the identity card. The following section outlines the elements of a secure ID system architecture, and how digital watermarking fits in this architecture.

A secure ID system architecture includes:

- Data capture
- Applicant verification (including identity source document verification)
- Secure ID production
- Secure and high quality ID card
- Inspection and verification of ID card and card holder

For example, even if the ID card is very secure, an authentic but invalid card can be obtained with falsified identity source documents during the applicant verification step.

Verification of identity source documents with digital watermarks

During the issuance process of a federal government ID card, I-9 Identity Source Documents are used to identify the applicant. These I-9 documents will be scanned and saved for issuance and auditing purpose, whether or not the card is issued to the applicant. Digital watermarks in these source/breeder documents, such as a driver license, birth certificate, passport, or social security cards, can be read during the scanning process to verify the document. There is no noticeable loss of throughput since the scanning process is slower than the digital watermark reading process. A supplemental white paper regarding this security feature can be provided, if requested.

"Chain of Trust" and Computer Access

Verifying the physical card, digital photo from the chip, and identity source documents via digital watermarking is just the beginning of providing a chain of trust. Digital watermarks can be layered upon each other to identify the "chain of trust" of any digital or printed document. For example, digital watermarks can also link any digital image or printed card to an owner or issuing equipment, such as a secure card printer, for forensic tracking purposes.

Furthermore, digital watermarks can be read using scanners, web cameras or cell phone cameras equipped with secure reader software. They can also be used for enhanced logical access to electronic information resources. For example, it may be useful in certain secure government facilities to enable PCs or terminals to read the digital watermark in the card as a requirement for logon.

Digimarc feels strongly that as the draft NIST standard for the secure personal identification verification process evolves, more applications for digital watermarking will emerge that improve security and enhance system performance.

CONCLUSION AND SUGGESTIONS

There are new challenges to creating secure identity documents because of counterfeiters' access to now ubiquitous digital computers, printers and scanners, and the proliferation of this powerful technology raises serious homeland security issues regarding identity documents. A security provider can use a whole system approach to address these threats by employing multiple document security layers which, in concert, provide a formidably enhanced solution. Identity documents that incorporate and rely solely upon chip data carriers provide a single focused point of attack, and, therefore, require additional non-chip based security features.

Digimarc recommends that the NIST standard includes a standard electronically readable code that links the physical card, digital photo on the chip, and the chip in a fixed field format of 96 bits. This electronic code provides a critical security layer to resist the data/photo alteration and substitution, wholesale counterfeit, and compromising the chip or reader attacks.

Digimarc suggests that the NIST standard recommend the usage of digital watermarking to provide this electronically readable code, as well as forensic data and identity source

document verification. Digital watermarks are resistant to attack, and any compromise requires diverse expertise in signal processing, communication theory and perceptual modeling. These fields of expertise are different than those required to attack the current digital and traditional print card security features, thereby raising the time and cost to compromise these credentials. The same digital watermarking techniques can also be used to verify the identity and authenticity of source documents, and to provide the complete "chain of trust" required for a truly secure ID system architecture.

ABOUT DIGIMARC

Digimarc Corporation (NASDAQ: DMRC), based in Beaverton, Oregon, is a leading supplier of secure media solutions used in a wide range of security, identification and digital media content applications. Digimarc provides products and services that enable the production of more than 60 million personal identification documents and driver licenses per year in 32 U.S. states and the District of Columbia and more than 20 countries. Digimarc's digital watermarking technology provides a persistent digital identity for various media content and is used to enhance the security of financial documents, identity documents and digital images, and support other media rights management applications.

Digimarc has an extensive intellectual property portfolio, with 180 issued U.S. patents with more than 3,000 claims, and more than 350 pending patent applications in digital watermarking, personal identification and related technologies.

The company is headquartered in Beaverton, Oregon, with other U.S. offices in Burlington, Massachusetts; Fort Wayne, Indiana; San Francisco, California; and the Washington DC area; and European offices in London. Please go to www.digimarc.com for more company information.

For more information, please contact:

ENHANCING PERSONAL IDENTITY VERIFICATION WITH DIGITAL WATERMARKS

DIGIMARC®

Tom Gann Vice President of Government Relations 1300 Connecticut Avenue, Suite 600 Washington, DC 20036 (Phone) (202) 496-2134 TGann@digimarc.com	**Garth Zambory** Director Business Dev., Secure ID Systems 9402 Cleat Court Burke, VA 22015 (Phone) 571-276-3930 (Fax) 703-455-7459 GZambory@digimarc.com