"Correlation System for Security Validation and Verification Using An Encoded Phase Mask"

FINAL SCIENTIFIC & TECHNICAL REPORT

Contract Number: F30602-97-C-0354
Data Item No.: A009

POP:

12/17/97 - 12/31/00

June 26, 2001

Prepared for:

Joseph L. Horner
Air Force Research Lab/SMHC
80 Scott Drive
Bldg. 1138, Rm 105
Hanscom AFB, MA 01731-3010

Prepared by:

David C. Weber and James D. Trolinger
MetroLaser, Inc.
18010 Skypark Circle, Suite 100
Irvine, CA 92614-6428
(949) 553-0688

REPORT DOCUMENTATION PAGE

Form Approved

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
06/26/01	Final Report	12/17/97 to 12/31/00

4. TITLE AND SUBTITLE

Correlation System for Security Validation and Verification Using An Encoded Phase Mask

5a. CONTRACT NUMBER

F30602-97-C-0354

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Weber, David C.
Trolinger, James D.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

MetroLaser, Inc., 18010 Skypark Circle Suite 100, Irvine, CA 92614-6428

8. PERFORMING ORGANIZATION REPORT NO.

TRL1DWF.DOC

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Lab/SNHC
80 Scott Drive
Bldg. 1138, Room 105
Hanscom AFB, MA 01731-2909

10. SPONSOR/MONITOR'S ACRONYM(S)

RL/EROP

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. SUPPLEMENTARY NOTES

13. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

14. ABSTRACT

Verification technologies are needed to confirm the identity of personnel and to validate the authenticity of manufactured products. Rapid advances in computers, printers scanners, and copiers have made it increasingly easy to reproduce security emblems traditionally used for verification and authentication. Even holograms, once considered impenetrable, are now routinely counterfeited using techniques such as holographic contact copying. To circumvent the effectiveness of intensity sensitive devices to copy traditional security emblems, the use of complex phase patterns has been proposed. An ID card is produced by bonding a phase mask to some primary identification pattern such as a fingerprint. A nonlinear joint transform correlator is then used to match the ID card to an identical phase mask that is part of an automated reader. However, such a phase encoded ID card could be copied by using innovative holographic techniques. To avoid this, MetroLaser has developed an innovative holographic technique that utilizes an ID card that is an inseparable combination of an information wavefront and another complex wavefront, both unknown to the potential counterfeiter. The two patterns on the card are deconvolved using a "Key" Hologram that is part of the reader, resulting in a nearly ideal security system.

15. SUBJECT TERMS

phase mask, security verification, holographic seal, fingerprint identification, biometrics

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			David C. Weber
Unclassified	Unclassified	Unclassified	SAR	46	19b. TELEPHONE NUMBER *(Include area code)* (949) 553-0688 x240

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39-18

TABLE OF CONTENTS

TABLE OF FIGURES

EXECUTIVE SUMMARY

The work covered in this report was conducted under an Air Force SBIR contract to develop an optical correlator that could be used in conjunction with a secure holographic ID card. The resultant automated identification system was targeted for use in secure entry applications necessitating the highest level of security.

One of the primary objectives of the program was the development of an optical card that would be extremely difficult to duplicate and would secure sensitive information in such a format as to preclude unauthorized viewing of its content. Specifically, the ID card was required to contain biometric information that acted as a local database which could be compared against the live biometric of the individual requesting entry. Since the system is only as secure as the database contained on the ID card, it is essential that the card be immune to reading, interrogation, alteration, or duplication.

To achieve these goals, MetroLaser developed a holographic ID Card based on a patented method of recording information holographically within the volume of an optically thick substrate. Properly conditioned and digitized biometric information was encoded and secured in the hologram card by producing the hologram with a complex reference beam (holograms are normally produced with a simple, easily-reproducible reference wave). Thus, information recorded in the hologram by the card writer could be released only when it was illuminated with the same complex wavefront used during recording. Since such a complex wavefront must be both precisely aligned to the Card Hologram and faithfully duplicated in multiple card readers, this "key" wavefront was itself stored in the form of a hologram that was in direct contact with the "Card" Hologram during recording and playback. Thus, the "Key/Card" Hologram pair was used to achieve the security requirements outlined in the previous paragraph.

A second objective of the program was to investigate the nature of the correlator itself, which would be used by the reader to compare live biometric information presented by an individual with the biometric information stored on the ID card. To this end, initial work was conducted toward the development of a Joint Transform Correlator (JTC). One of the main strengths of the JTC is that it can quickly correlate two complex signals with a high degree of discrimination. The JTC is also relatively robust and easy to align as compared to other methods such as matched filters.

The use of a JTC as an ID card reader, however, requires the use of a relatively expensive SLM and precise initial alignment. Its hardware and fabrication costs are, therefore, high compared with electronic card readers currently used in commercial security applications (i.e., Smart Cards). Also, many biometrics currently in use (e.g., fingerprints) can be reduced to a relatively small data set that does not require the speed or accuracy of the JTC. Since the fingerprint is currently the most familiar and used biometric in security applications, we adopted this biometric for the initial implementation of the Key/Card system. These considerations led us to pursue, as a first step, a more simplified implementation of the correlator for the Air Force system. The JTC ultimately will permit the use of more complex biometrics such as face or iris recognition, as well as combined biometrics. As security requirements evolve and become more demanding, implementations that have data capacity requirements that exceed current electronic Smart Card capabilities will be well suited for the JTC concept.

The fulfillment of the two program objectives cited above were accomplished through the successful construction of a Phase II prototype system. A holographic card reader and writer were developed and tested that implemented MetroLaser's patented "Key/Card" Hologram concept to store and retrieve biometric information from a secure ID Card. Both the Key and Card Holograms were recorded on an optically thick photopolymer film produced by Dupont. The Card Hologram was read indirectly through the use of a Key Hologram contained in the reader. The Key Hologram consisted of two collimated

wavefronts that impinged the hologram at different angles. More complex wavefronts were tested during the Phase II effort, but were not implemented in the prototype system.

The holographic card writer incorporated a commercially available fingerprint reader manufactured by Saflink Corporation that utilizes a solid-state sensor made by Veridicom, Inc., a spin-off of Lucent Technologies. The Saflink routines convert a fingerprint into a binarized code that is 400 bytes or less in length. An SLM is then used to convert this fingerprint code into an optical wavefront. Optics were then used to re-image this amplitude-modulated wavefront near the hologram material. This de-focused information wavefront was recorded in a hologram by combining it with a reference beam.

The holographic card reader implemented a method of writing and reading fingerprint data in a reduced data set that allowed direct comparison between the card information and the live fingerprint. Using this reduced code set, the card reader was able to successfully read the biometric code and correlate this information with that produced by a live fingerprint. A Key Hologram contained in the reader was used to release the biometric code contained in the Card Hologram. The reader is an extremely simple and compact system, consisting of only a light source (diode laser), two beam-expanding lenses, a mirror, the holograms, and a detector array. The package dimensions are approximately 8" x 8" x 4". The reader was tested to verify that it could positively identify an individual whose fingerprint code was contained on a MetroLaser ID Card. Limited testing was also done to demonstrate that another user could not use this same card to produce a positive result.

Each "bit" of the biometric code was viewed optically by the reader using a 4 x 4 pixel area of a CCD camera. Because CMOS (Complementary Metal Oxide Semiconductor) detectors potentially offer a much lower cost solution, a CMOS detector array was also tested, but not used in the final implementation because of the lack of access to the manufacturers software. Using a data bit size of 16 camera pixels, the detector was able to read a 400-byte fingerprint code using approximately 50,000 pixels. Additional bits were used to provide error correction. As the bit area is reduced, the data density increases, allowing additional information to be stored on the card (e.g., additional fingerprints or more complex biometrics). One important extension, as data capacity is increased, will be the addition of encryption keys used in public-private key (PKI) Internet security applications.

In conclusion, a secure method of storing and retrieving biometric information on an ID card was developed during this program. In fulfillment of the stated Phase II proposal objectives, a prototype card reader and writer were constructed and successfully demonstrated, including a method of introducing and reading secure biometric information on a holographic ID card. We are currently looking for applications niches and potential investors for a Phase III program. Additional developments for commercial applications such as Internet security are also under discussion. We are also continuing to investigate the practical engineering issues and refinements identified during Phase II.

DESCRIPTION OF PROTOTYPE SECURITY SYSTEM

The Phase II effort culminated in the construction of a holographic card reader and card writer that were used to produce and retrieve biometric information for the purpose of verifying the identity of the cardholder. In this section, the features and other details of the system will be presented.

Photographs of the holographic ID card writer are shown in **Figure 1** and **Figure** 2. A diode pumped, frequency doubled YAG laser was used in conjunction with a beamsplitter to produce the reference and data wavefronts required to produce the Card Holograms. Each of the two wavefronts was expanded, collimated (lens L1 or L4), and passed through an iris to produce wavefronts that were nominally planar. **Figure 3** and **Figure** 4 show close-ups of the Spatial Light Modulator (SLM) and other system components while the system was under development in the laboratory.

To create the data wavefront, the user's fingerprint was first read using a fingerprint reader manufactured by Veridicom, Inc. The software next digitized this information into a condensed code of 300 to 400 bytes. This digitized code was then displayed on the SLM, seen in more detail in **Figure 4,** and was used to modify the Data Wavefront as it passed through SLM. Polarizers before and after the SLM were used to produce a binarized amplitude wavefront. The image produced by the SLM and later read by the CCD contained in the holographic card reader is shown in **Figure 5**. An image of the Data Wavefront leaving the SLM was produced about an inch behind (beyond) the hologram itself through the use of two matched lenses, L2 and L3. Projecting the digitized information in a plane other than the hologram plane was used to add an additional layer of security to the data, since it is more difficult to view without the proper reconstruction wavefront.

The encoding reference beam, as shown in these figures, was a simply collimated wavefront that was reproduced in the reader using the Key Hologram. The full implementation of the Key/Card concept can be realized with this same instrument by inserting a phase mask, which could be an additional SLM or fixed mask, after the lens, L4. As more complex encoding wavefronts are used in both the Key and Card Holograms, alignment between the two becomes more critical. Alignment issues were addressed and partially resolved during the Phase II program, but were not included in the Phase II prototype demonstration.

The card writer SLM and the fingerprint reader were interfaced into a personal computer (PC). During registration the software controlling the writer displayed a screen that prompts the user to insert a blank card into the writer and his finger onto the fingerprint reader. A photograph of the screen that is displayed after the user fulfilled these requirements is shown in **Figure 6**.

The card produced using the holographic card writer contained the necessary digitized fingerprint information for the holographic card reader to verify the user's identity. The prototype card reader produced for the Air Force during the Phase II program is an extremely simple and compact device that interfaces directly into a PC via a frame-grabber. The frame-grabber is used to read images produced by the CCD array contained inside the reader. The Veridicom fingerprint reader is also interfaced with the same PC and used in conjunction with the holographic card reader to identify the user. A photograph of the card reader is shown in **Figure 7** with a card inserted into a slot located on top of the reader. **Figure 8** shows two photographs of what is contained inside the reader. Labels are shown indicating the laser, microscope objective, collimating lens, Key Hologram, and CCD array that make up the system.

The program used to verify the cardholder's identity is contained in a file named MLHSReader.exe. To verify the cardholder's identity, the user inserts his/her card into the reader and clicks a "Verify" button as directed. The system asks the user to scan his/her finger and compares the live data with that contained on the holographic ID card. If data between the two matches, the system will display "MATCH" as show in **Figure 9**. Otherwise, the system will continue scanning to see if it can find a correlation between the live fingerprint and the digitized information encrypted into the holographic identity card.

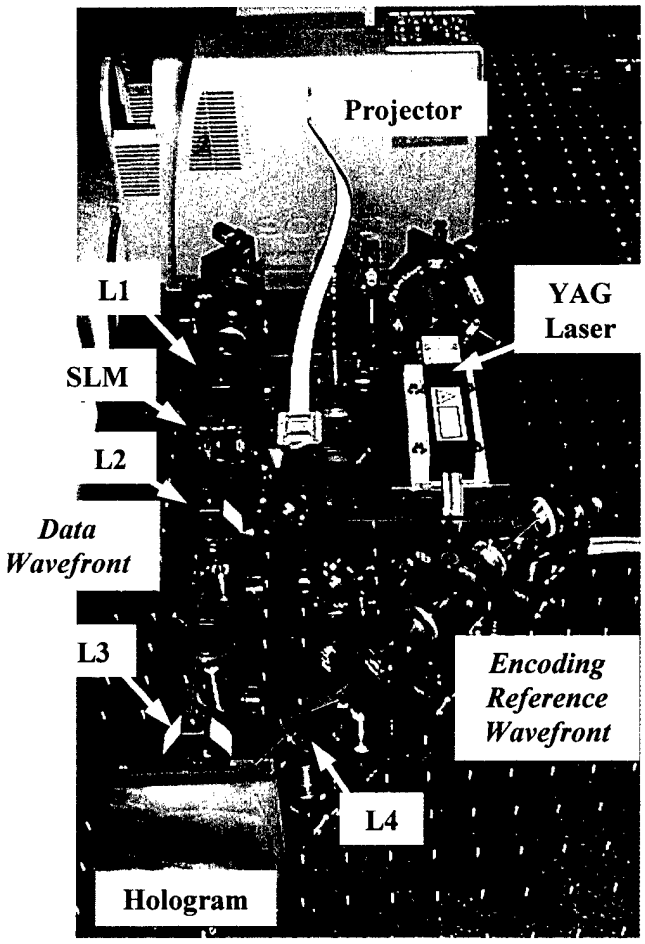


Figure 1. Photograph of holographic card writer showing object and reference beams used to create holographic image of biometric data.

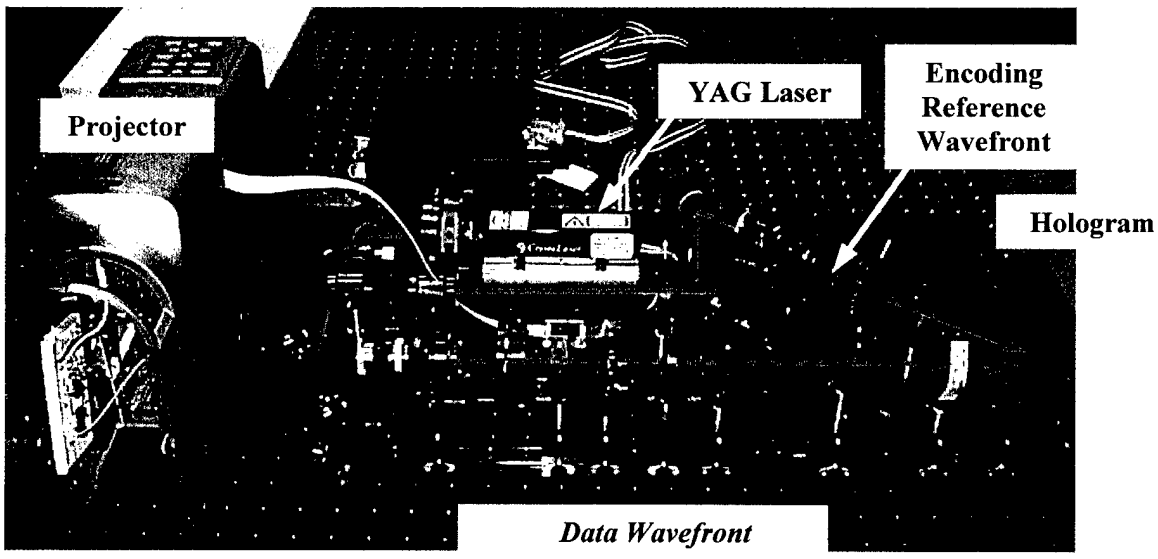


Figure 2. Secondary view of holographic card writer.

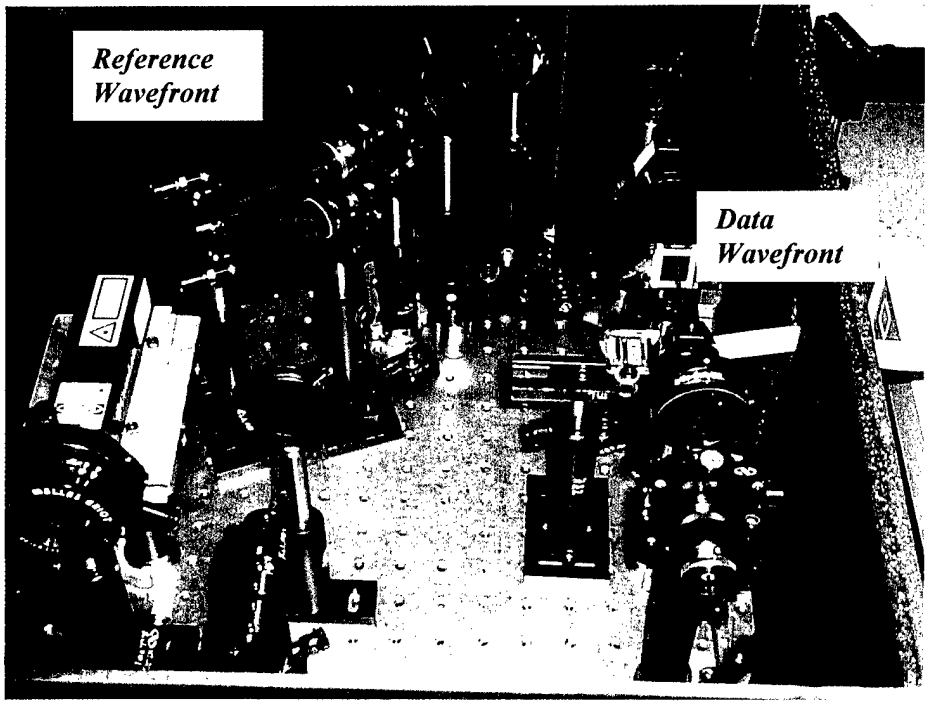


Figure 3. Close-up view of holographic card writer during laboratory development.

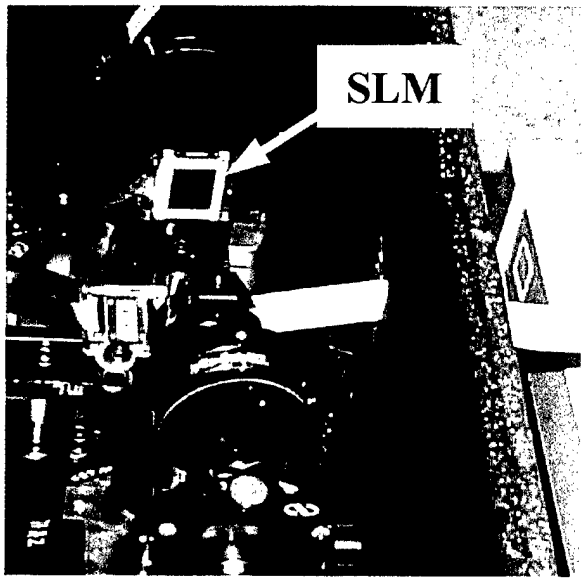


Figure 4. Close-up view of SLM used in holographic card writer.

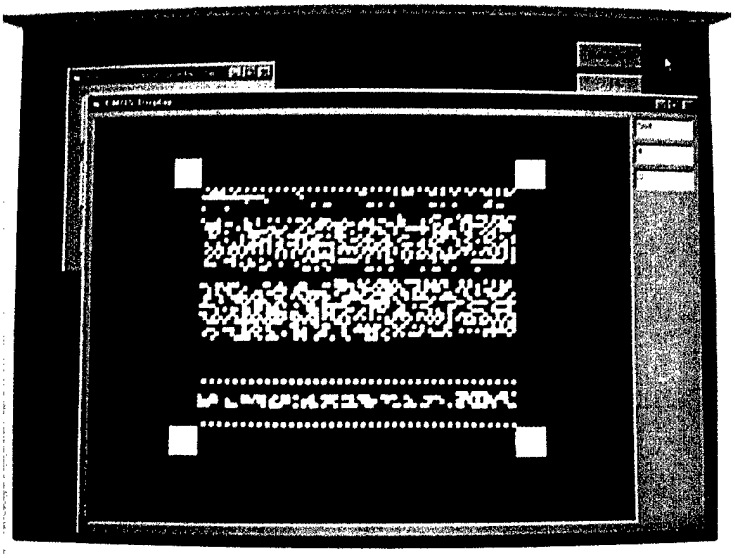


Figure 5. Binary image representation of fingerprint recorded on holographic ID card. Squares in four corners of image are used for registration during playback of holographic image into CCD array.

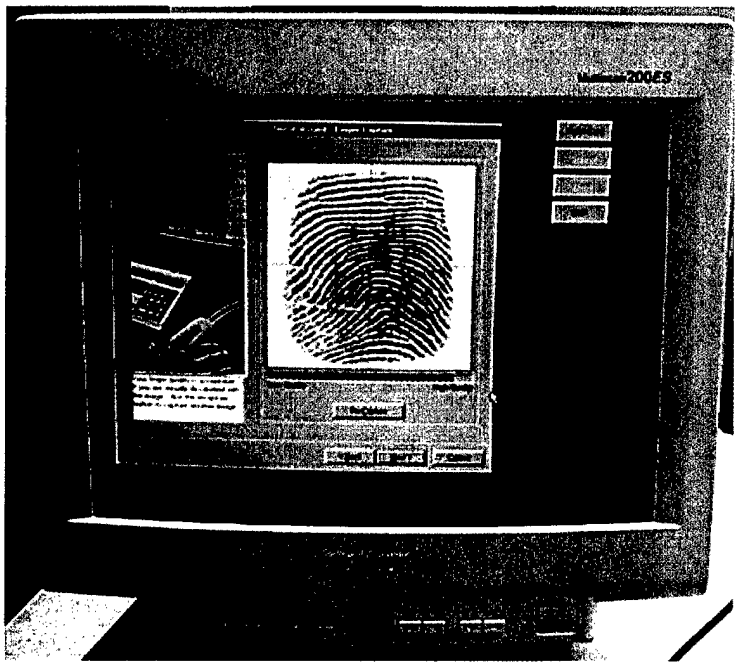


Figure 6. Input screen for registration of fingerprint.

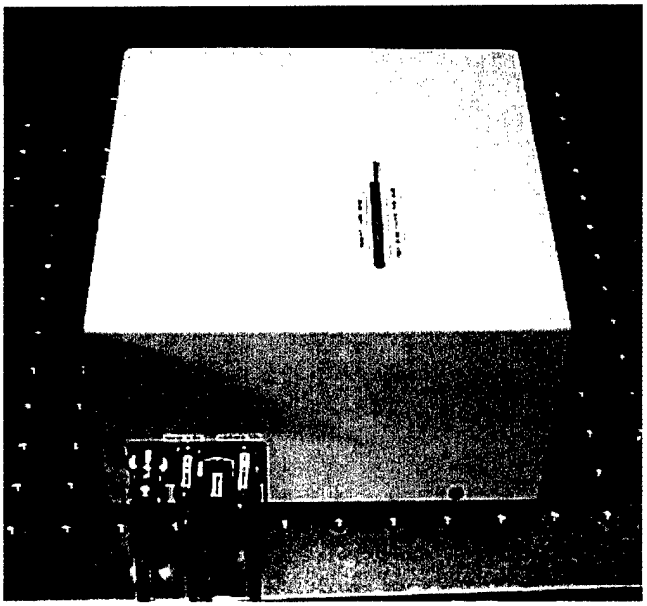


Figure 7. Photograph of holographic card reader used to confirm the identity of the cardholder. Holographic card shown inserted into slot on top of reader.

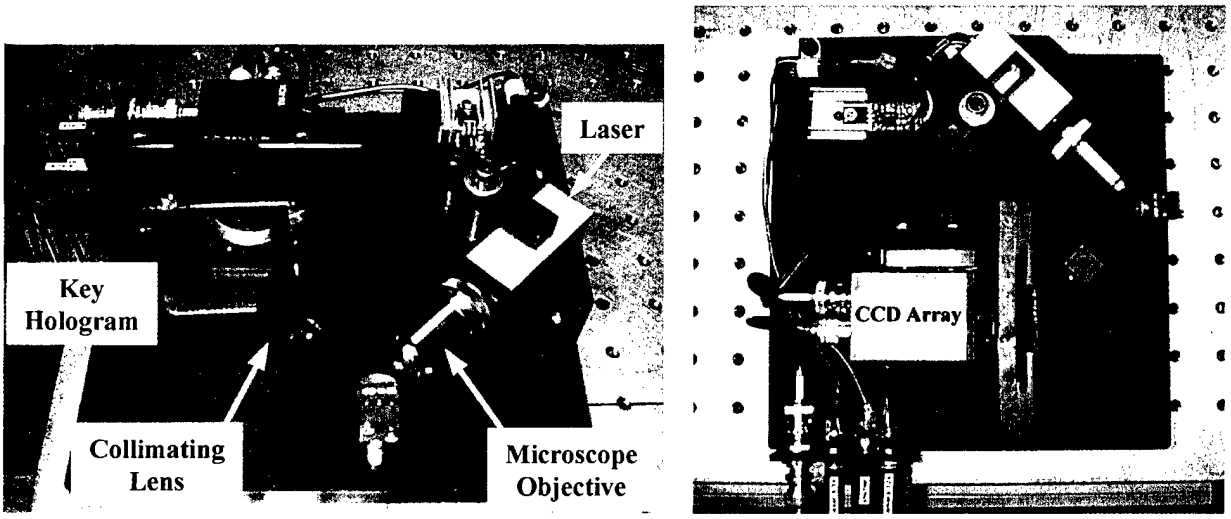


Figure 8. Perspective and top views of the insides of the compact holographic card reader developed for the Air Force during the Phase II program.

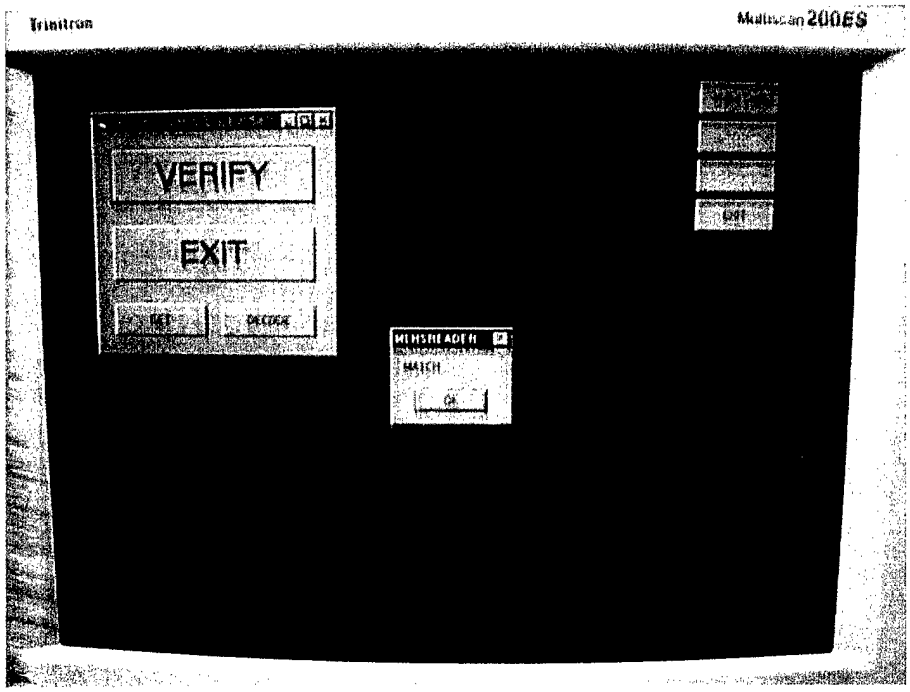


Figure 9. Screen of result when a successful match is made between the live fingerprint and the holographic ID card.

PROGRAM BACKGROUND

Tamper-proof verification technologies are desperately needed in both the military and commercial sectors to accurately and efficiently confirm the identity of a person, as well as to validate the authenticity of manufactured products. In the military realm, access to secure areas and sensitive information through passes or ID cards is an important application. In the commercial sector, estimates are that 30% of all world trade is counterfeit.[1] In some cases, the manufacturer (and honest consumers) are the only injured parties, yet in other cases, such as the medical field or aircraft engine parts, major public health and safety risks are involved. Credit card fraud is another serious problem that affects banks, businesses, and the card carrier.

To circumvent the effectiveness of intensity sensitive devices to copy traditional security emblems, Javidi and Horner have suggested a scheme of complex phase/amplitude patterns that cannot be seen under normal lighting nor reproduced by devices such as copiers or CCD cameras.[2] In this approach, an ID or credit card would be produced by permanently and irretrievably bonding a phase mask to a primary identification amplitude pattern such as a fingerprint, a picture of a face, or a signature. The biometric information contained on the card is verified by either a device or inspector, while the authenticity of the ID card itself is verified by the automated comparison of the phase mask on the ID card to a reference mask containing the same phase information. Computer simulation results and tests by Javidi on this approach have verified that both the phase mask and primary pattern are identifiable in an optical processor or correlator.[3] While various options exist for the optical correlator, the use of a nonlinear joint transform correlator (JTC), like that seen in **Figure 10**, has been shown to give the best performance in correlating two such phase masks.[4] While such a phase-encoded ID card cannot be copied using traditional, intensity-sensitive devices, interferometric or holographic techniques can be used by more sophisticated counterfeiters to obtain the phase information and thereby produce unauthorized copies. In past work by MetroLaser, an innovative holographic concept has been demonstrated, referred to as a Key/Tag Hologram, that prevents unauthorized access to either the phase or the amplitude information contained in an ID card or tag. The content of a Tag Hologram can only be obtained when illuminated with the same complex wavefront used to make it. This complex wavefront for reading the ID card is provided by the Key Hologram, which is used, in essence, to "unlock" it.

Rather than using a phase mask directly, the MetroLaser technology will be used to encode the information in the form of a "Card" Hologram containing the desired phase and amplitude information. A "Key" Hologram, which is an integral part of the reading device, will unlock (decode) the complex wavefront to be compared with the reference phase mask in the optical correlator. The recording and playback procedures are shown in **Figure 11** and **Figure** 12. The ID card is now an inseparable combination of the complex correlation signal and another complex wavefront, the nature of which would be unknown to the cardholder or potential counterfeiter. Without knowledge of the content of the complex decoding beam, it is extremely difficult to determine the content of the phase mask.

The Key/Card Hologram represents what could well be the ultimate in securing the content of an ID card against either unauthorized duplication or falsification. The only way to obtain the content of the ID card and thereby copy and/or modify its content is to illuminate it with the complex wavefront used during recording. This now moves the control problem from the ID cards (of which there are many copies held by many individuals), to the Key (of which there are few copies) which would be mounted inside machines located in secured areas. The Key can be mounted in the reader in such a way that it self-destructs if removed.

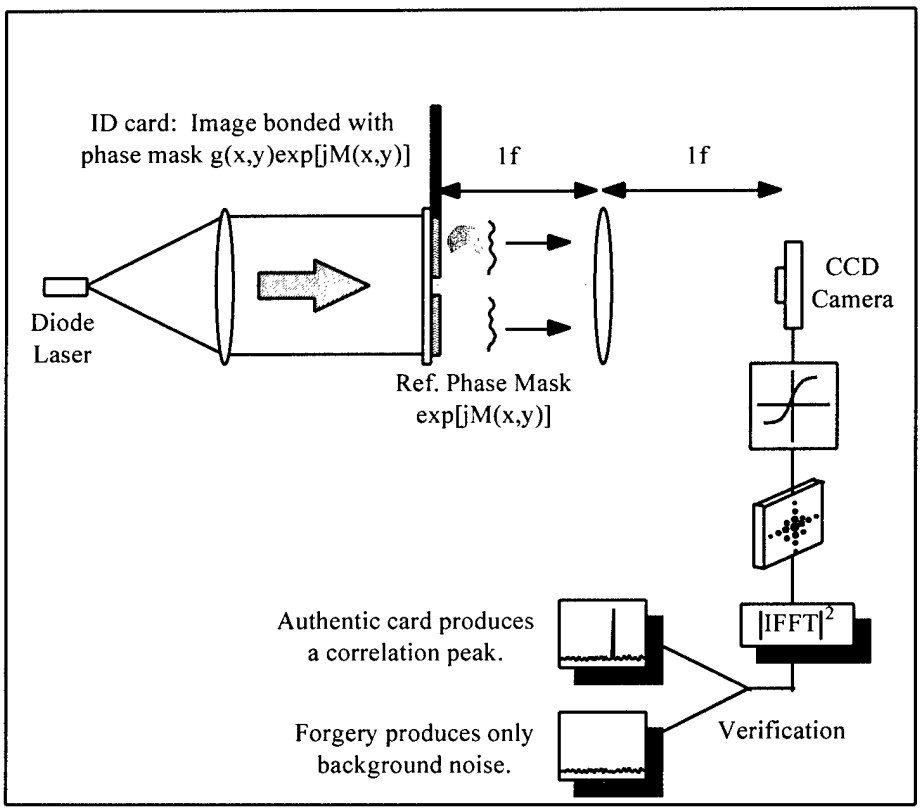


Figure 10. Nonlinear joint transform correlator for verifying a fingerprint match in addition to verifying the authenticity of the phase mask superposed over the fingerprint on an ID card.

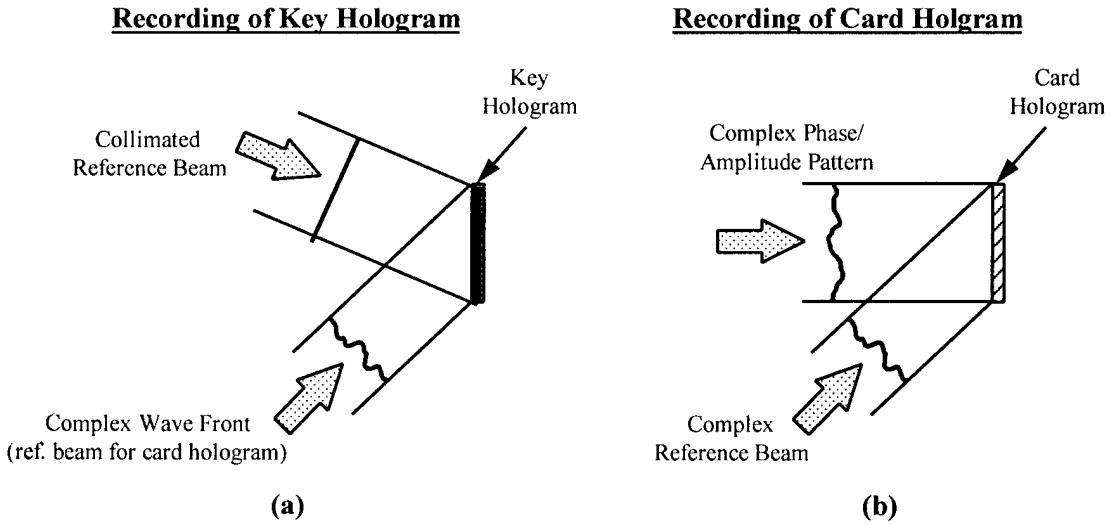


Figure 11. Use of Key/Card approach in making a phase mask that cannot be copied using phase recording techniques such as contact copying.

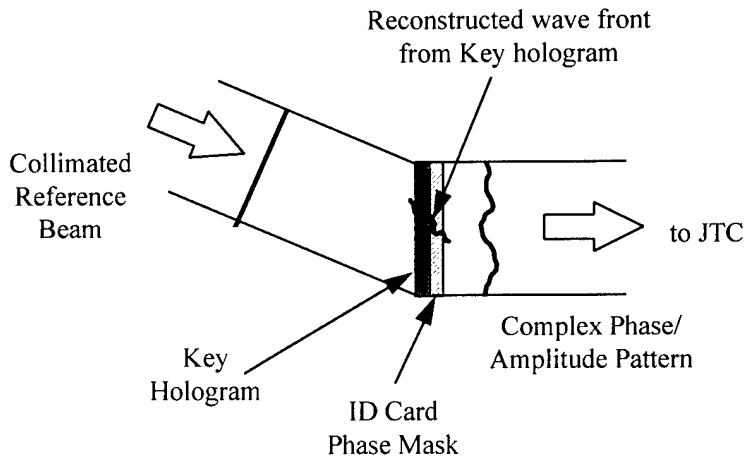


Figure 12. Reading the phase mask on ID card using the Key Hologram.

The original concept of the reader for the Key/Card Hologram ID card was to utilize a JTC as a method of comparing the content of the card with information used to confirm the identify the cardholder. One of the main strengths of the JTC is that it can be used to quickly correlate two complex signals with a high degree of discrimination. While the JTC is relatively robust and easy to align compared to other methods, such as matched filters, the cost of the hardware required to incorporate this technology into a card reader is relatively high as compared to electronic cards (Smart Cards) that could be used as a less secure solution to the Air Force problem of positive, automated identification for secured entry.

The JTC allows the reader to compare two complex signals, such as the images of two similar fingerprints or other type of biometrics, and quickly determine their degree of similarity. Most biometrics, however, can be reduced to a much smaller data set that accurately describes the unique features involved. This reduced data set is usually somewhere between a few bytes to as much as 1 Kbyte, depending on the complexity of the biometric and the description accuracy required. Fingerprints, for instance, are described using commercially available systems with around 300 bytes. These systems also utilize robust algorithms that reliably compare two such fingerprint codes in the presence of noise to determine if they were generated from the same finger.

A simpler, digitized version of the biometric information stored in the ID card can, therefore, be utilized to eliminate the necessity of using a JTC and an SLM to obtain fast, accurate comparisons between a live fingerprint with one stored in an ID card. The result is a reader/ID card system that is no less secure than the JTC version, but which utilizes a reader that is much less expensive. Such an approach would also offer the potential of competing with Smart Card solutions in the commercial marketplace.

A concept drawing of the reader system that was ultimately developed at MetroLaser to solve the Air Force problem is shown in **Figure 13**. The biometric information contained on the Card Hologram is reduced to a binary code that can be directly read by a CCD or inexpensive CMOS detector array. This type of compressed format of the biometric information is used by a number of commercial fingerprint systems currently marketed for use on PC's. The compressed fingerprint code is digitized and stored on the hologram during enrollment through the use of a spatial light modulator (SLM) in which each pixel or set of pixels represents one bit of the digitized code. During presentation, the digitized representation from the fingerprint reader used at the point of entry into a secured area is compared to the information stored in the encrypted Card Hologram.

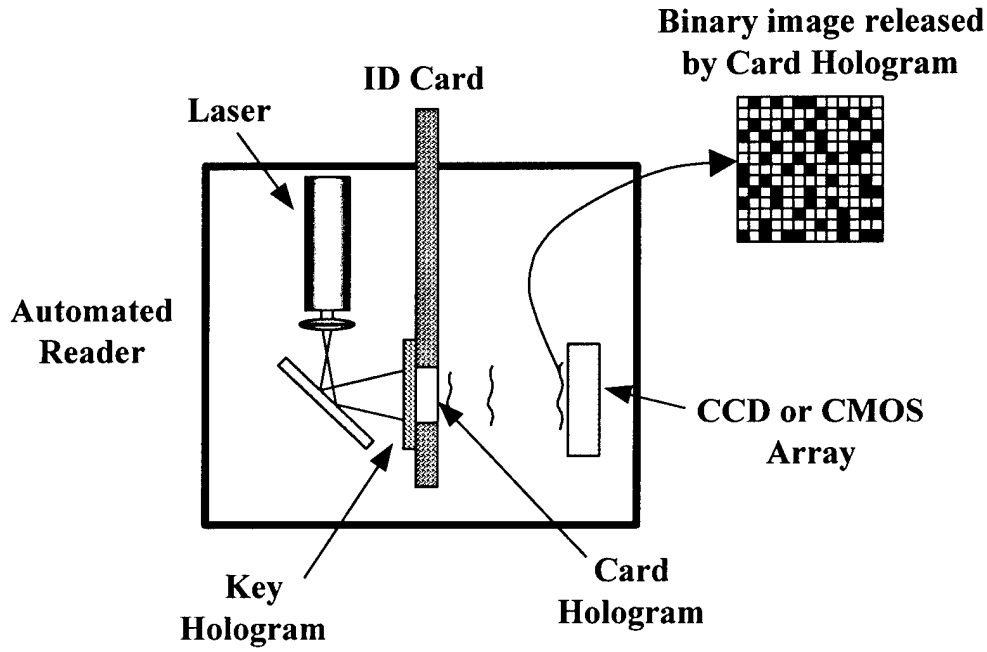


Figure 13. Conceptual layout of a reading machine used to release digitized biometric information contained in a Card Hologram.

LABORATORY WORK

An extensive laboratory effort went into addressing technical issues related to the development of the Phase II prototype system. These issues were reported to the Air Force in the form of quarterly reports and are summarized in the following sections.

BR-Based Fingerprint Correlator

Various studies were conducted during the course of the Phase II program to investigate the use of a photochromic material referred to a Bacteriorhodopsin (BR). A breadboard system of a BR-based optical correlator was investigated for fingerprint identification. The setup for the all-optical correlator is shown in **Figure 14**. The laser beam from an Argon-Ion laser (514 nm) passes through a spatial filter and beam expander, and is divided into three beams with a pair of beamsplitter cubes. The two 'writing' beams pass through the two images to be correlated, which are introduced onto photographic negatives. The third beam is used as a 'high-pass' filter in the Fourier plane, as will be discussed below. A lens Fourier transforms the two images, producing an interference pattern in the BR. A Helium-Neon laser is then used to read the recorded information, producing a diffracted signal on the photo detector. During these experiments, a simple BR film was used in the Fourier Transform plane. In future implementations, a BR spatial light modulator will be used to enhance the diffraction efficiency and signal-to-noise ratio.

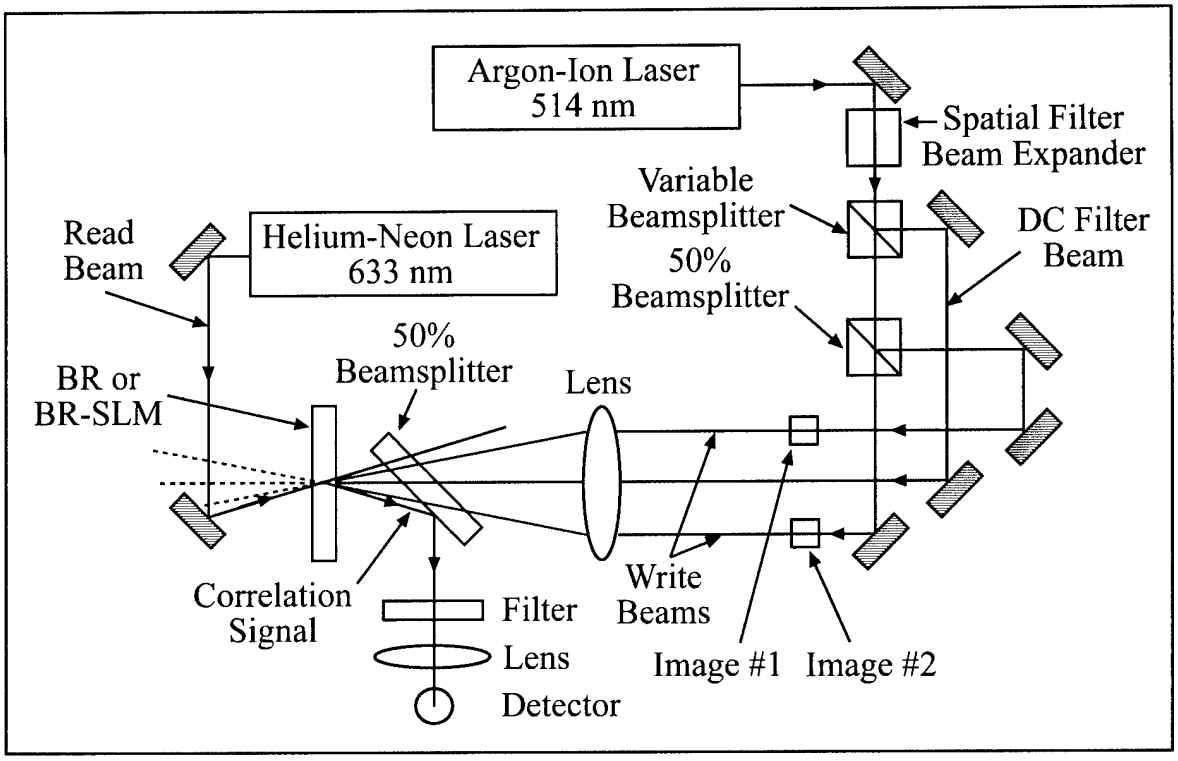
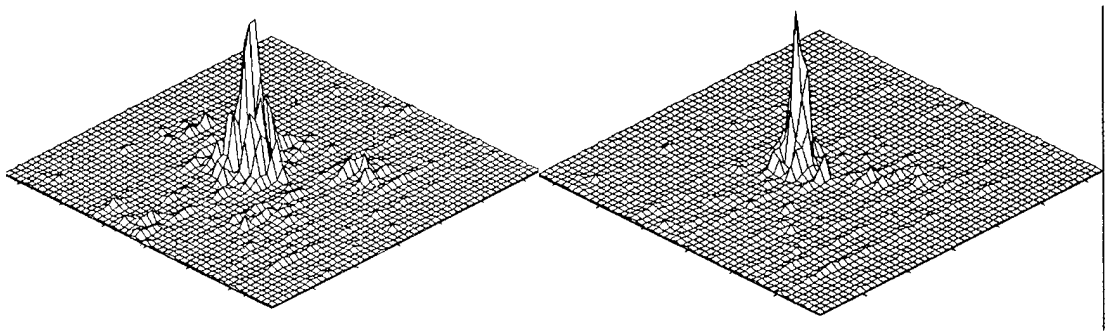


Figure 14. Joint Transform Optical Correlator with BR film.

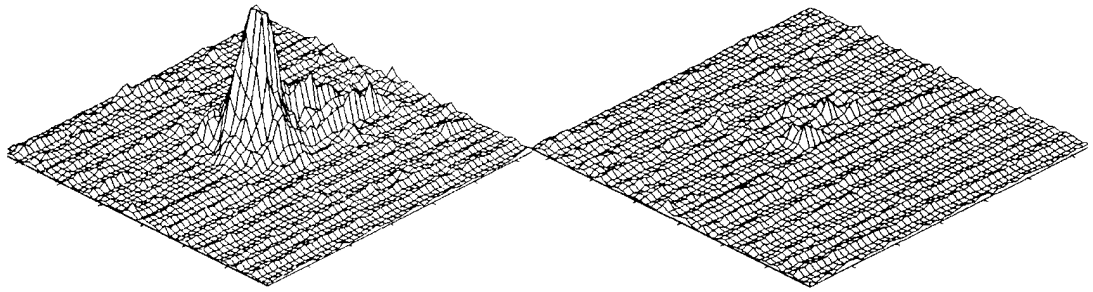
The optical correlator was first characterized by correlating two identical laser beams (no images). Several experimental parameters were adjusted in order to maximize the diffracted signal, such as the power in the read and write beams, and the angular separation of the write beams. The diffracted signal was seen to be linearly proportional to both the read and write beam powers, and the signal increased with the angle between the write beams. The data shown below used 30 mW at 514 nm for the write beams, 8 mW at 633 nm for the read beam, and the write beams were separated by 25 mm, producing an angle of about 7°.

The BR-based correlator showed promising results in the discrimination of fingerprints. These results were greatly enhanced, however, by adding a second beamsplitter to create a third laser beam in the experimental setup. This third beam was focused with the same lens, producing a focused spot in the center of the Fourier transform (spatial frequency) plane. By increasing the intensity of this beam, the BR film can be locally saturated at this location in the frequency plane, effectively blocking that frequency component. The addition of the third beam acts as a "high pass" filter in the frequency spectrum. Experimentally, this frequency filtering produced a dramatic improvement in the correlation results. **Figure 15** shows the correlation between two identical images, for the cases of two beams and three beams. Although the absolute magnitude of the correlation peak is reduced by the presence of the third beam, the peak sharpness and signal-to-noise ratio is significantly better. When comparing two different images (i.e., two different fingerprints), the addition of the third beam definitely improves the correlation result. **Figure 16** shows the correlation for the two and three beam cases. Clearly, the three beam result shows that the two images do not match, while the two beam case still shows a great deal of correlation. The system has been tested with several fingerprints, and the correlator successfully identified all matches and rejected all mismatches in the three-beam mode. These results will be reported more quantitatively in future reports.



a) b)

Figure 15. Optical correlation of two identical fingerprints: a) two beams; b) three laser beams.



a) b)

Figure 16. Optical correlation of two different fingerprints: a) two beams; b) three beams.

Key/Card Hologram Development

An experimental breadboard setup, shown in **Figure 17**, was constructed and used to address the technical issues associated with the development of the Key/Card technology. In order to analyze the output from the Key/Card Hologram, a signal received by the CCD was sent to a frame-grabber and software was developed in LabView™ to produce an electronic JTC.

The schematic in **Figure 17** shows the three beams necessary to produce the Key and Card Holograms. During recording of the Key Hologram, L1 and L2 are used to re-image Phase Mask 1 in the hologram plane. Iris 1 is used to control the frequency content of Phase Mask 1 that is recorded by the hologram. This entire leg can be translated to produce a live beam (Beam 4; dotted lines) that is compared to an earlier holographic recording of the same phase mask. A similar re-image arrangement is also used for the encoding phase mask (Beam 2). The setup is being used to perform a number of functions in the investigation of the Key/Card Holograms:

1. *Record Card Hologram* - Beams 1 and 2 are used to produce the encoded hologram to be used in the ID card.
2. *Record Key Hologram* - Beams 1 & 3 are used to record the Key Hologram that will be used in the reader to release Beam 2 from the Card Hologram. This is accomplished by illuminating the Key Hologram with Beam 3 (a simple read beam). The reconstructed Beam 1 is then used to reconstruct Beam 2 in the Card Hologram.

3. *Produce a live, translated image of the Mask 1* - Mask 1, L1, L2, and Iris 1 can all be translated together, normal to the direction of propagation (Beam 4). This live beam can be compared to the holographically recorded version of Mask 1 to compare the degree of correlation between the two.
4. *Perform a JTC between Mask 1 and the Card Hologram of Mask 1* - The Card Hologram is illuminated with Beam 2 (the encoding beam) and compared with Beam 4 (the translated signal from Mask 1). This allows us to examine the quality of the Key Hologram directly to assure that vital information was not lost during recording of the hologram.
5. *Perform a JTC between Mask 1 and the combined Key/Card Hologram signal* - The Key Hologram is illuminated with Beam 3 (simple, collimated wavefront). The output from the Key/Card combination is then compared with Beam 4 to determine the quality of the two-step reconstruction.

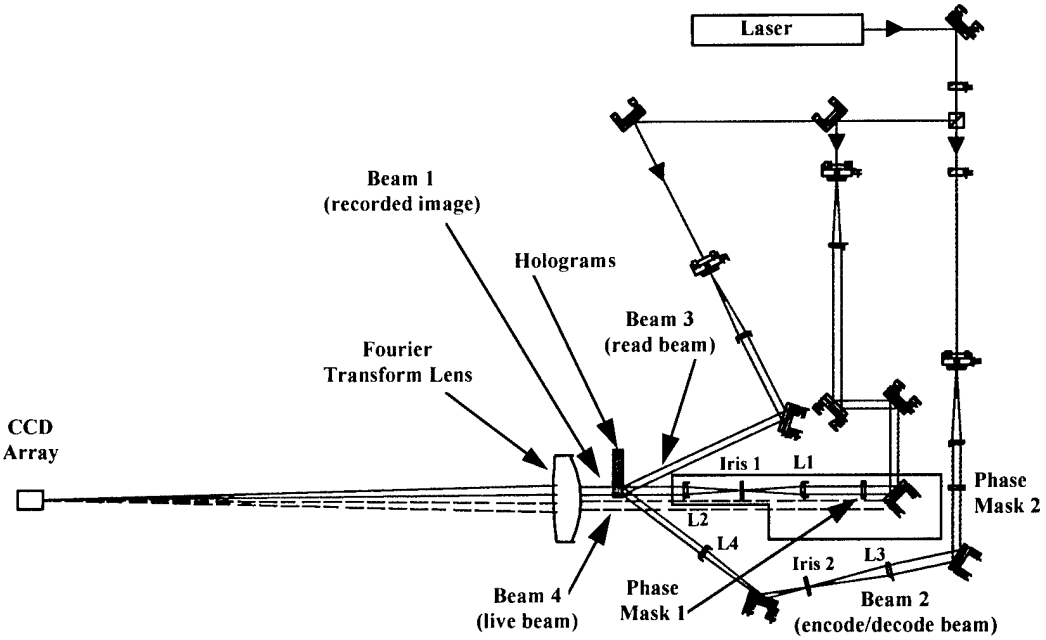


Figure 17. Experimental setup used to produce Key/Card Holograms of a random phase mask and to compare Key/Card recording of the mask to the live mask image.

Photographs of this breadboard setup are shown in **Figure 18** and **Figure** 19. This setup was used to successfully produce a Key/Card Hologram that produces a signal which can be correlated with the live image of the phase mask previously recorded on the Card Hologram. Results for correlation between the Key/Card signal and the live mask are shown in **Figure 20**. The top set of figures is two plotting formats of the same correlation signal resulting from this comparison. The number in the box on the left plot gives the magnitude of the correlation peak.

In the bottom set of figures, a small amount of random phase noise was added to one of the signals, which resulted in a decrease in the correlation signal. The change in the signal in the detector plane was imperceptible to the eye. This simulates what might be considered a "good" attempt at forging the Card Hologram contained on an ID card. Notice that the correlation signal is reduced by more than a factor of 4.

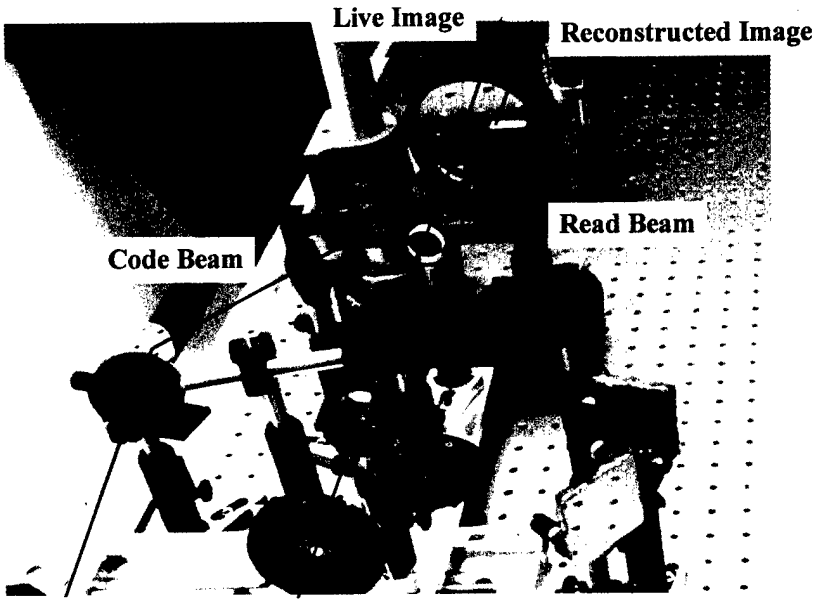


Figure 18. Close-up of experimental breadboard to record, read, and evaluate Key/Card Holograms.

Figure 19. Overall view of experimental breadboard to record, read, and evaluate Key/Card Holograms.

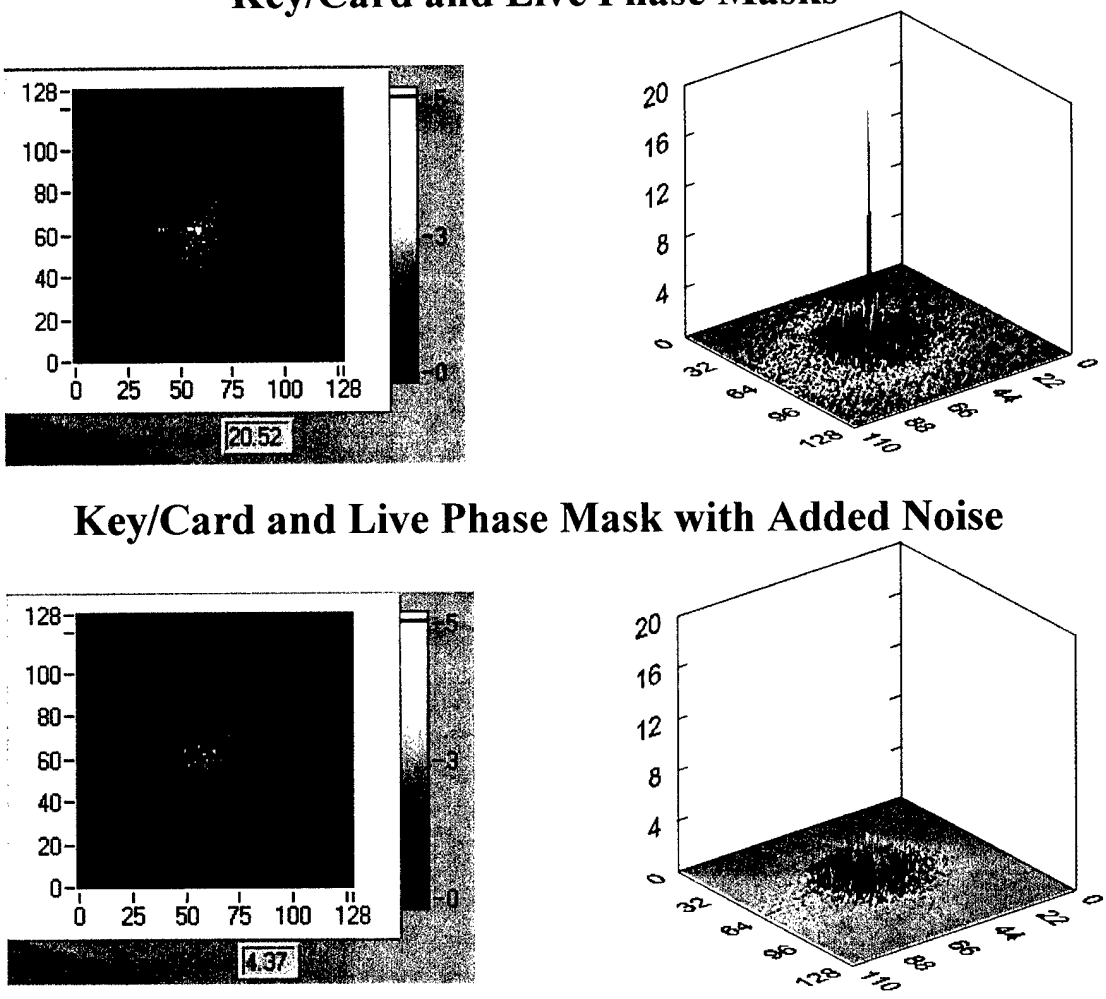


Figure 20. Correlation signal between a phase mask and its Key/Card holographic recording.

Use of Elongated Speckle to Reduce Alignment Sensitivity

The encoded Card Hologram discussed in the previous section was made by combining an encoded reference wave with an object wave containing the signal wavefront that would later become one of the inputs into a JTC or some other type of correlator. During the course of this work, it was found that when the encoded reference wavefront was sufficiently complex to prevent reconstruction of the signal with a simple collimated beam, alignment of the hologram became extremely critical. To achieve the required registration of the hologram with the encoded reconstruction wavefront, the hologram holder was mounted to a two-axis translation stage and carefully positioned relative to the decoding reconstruction beam.

Since this type of alignment would be impractical in a field system, a one-dimensional encoded wavefront was considered as a way to reduce critical alignment to one axis. Under this format, the card would slide past a 1-D reconstruction beam and, at some point, move into the correct position to reconstruct the signal wavefront.

To create the desired 1-D speckle pattern for the encoding reference wave, a cylindrical lens was used to focus a collimated beam onto the diffuser to create a horizontal line in the diffuser plane. Another cylindrical lens was used after the diffuser to collimate the resulting speckle wavefront in the vertical direction. This resulted in a beam with vertically elongated speckles at the hologram plane. The two-axis translation stage, to which the hologram holder was attached, was used to evaluate the alignment sensitivity of the decoding reconstruction wave relative to the hologram.

One of the LabView™ interface screens used during this testing is shown in **Figure 21**. As new images were acquired, the program displayed a running sequence of the correlation peaks, as well as their average value and standard deviation. In addition, other statistics of the image and the correlation were measured, such as the total energy in the image and the total energy in the correlation signal. The image, correlation image, and the correlation peak data could be saved to a file.

An inverse FFT was applied to the CCD image in order to calculate the correlation function. The JTC was used to evaluate the alignment sensitivity of the Card Hologram. The results of this investigation are seen in **Figure 22**, which shows the variation of the correlation peaks as the Card Hologram is moved to different horizontal and vertical positions relative to a one-dimensional decoding reconstruction wavefront. An expanded view of the horizontal axis only is shown in **Figure 23**. As can be seen from these figures, the alignment is much more sensitive in the horizontal direction. The card can be moved over a range of about 700 μm (approximately $1/32^{nd}$ of and inch) in the vertical direction before the correlation peak falls to about 80% of its aligned value. In the horizontal direction, the 80% range reduces to a motion of about 20 μm. By using a more structured diffuser to elongate the speckle pattern and better collimation methods, the sensitivity to misalignment in the vertical axis can be reduced even further.

The object wave of the encoded hologram in these experiments consisted of a diffuser to which a transparency of a fingerprint was attached. The diffuser and fingerprint were re-imaged about two inches beyond the hologram plane. The mask and fingerprint were re-imaged out of the hologram plane in order to secure this information from interrogation by simply illuminating the hologram with a collimated beam. In the previous paragraph, the security of the phase mask was demonstrated by the fact that a correlation with the reference mask could only be obtained by correct alignment of the hologram with its encoded reference wave. In **Figure 24**, it can be seen that the fingerprint information cannot be reconstructed without the same precise alignment in the horizontal axis. This figure shows that a misalignment of only 40 μm caused the image of the fingerprint to completely disappear.

Figure 25 shows that the image of the fingerprint remains even with misalignment in the vertical direction of a millimeter. The hologram was also illuminated with a simple collimated beam, in which case, the correlation function was reduced significantly, and the image of the fingerprint was completely gone.

These results show that both the biometrics and the phase information are protected when the hologram is illuminated by anything other than the correct decoding wavefront. A Key Hologram is currently being produced that will produce this decoding wavefront to release the information contained in the Card Hologram.

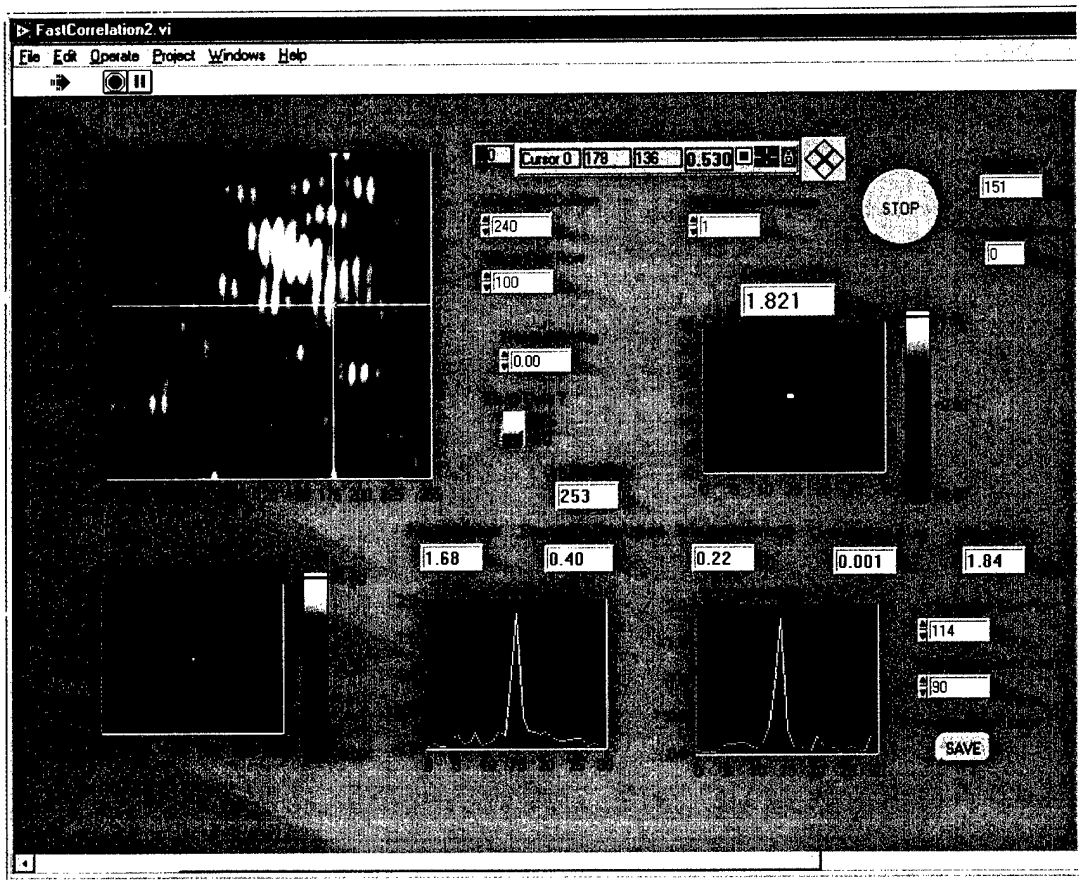


Figure 21. Typical user interface screen used in the laboratory JTC being used to evaluate the Key/Card Holograms.

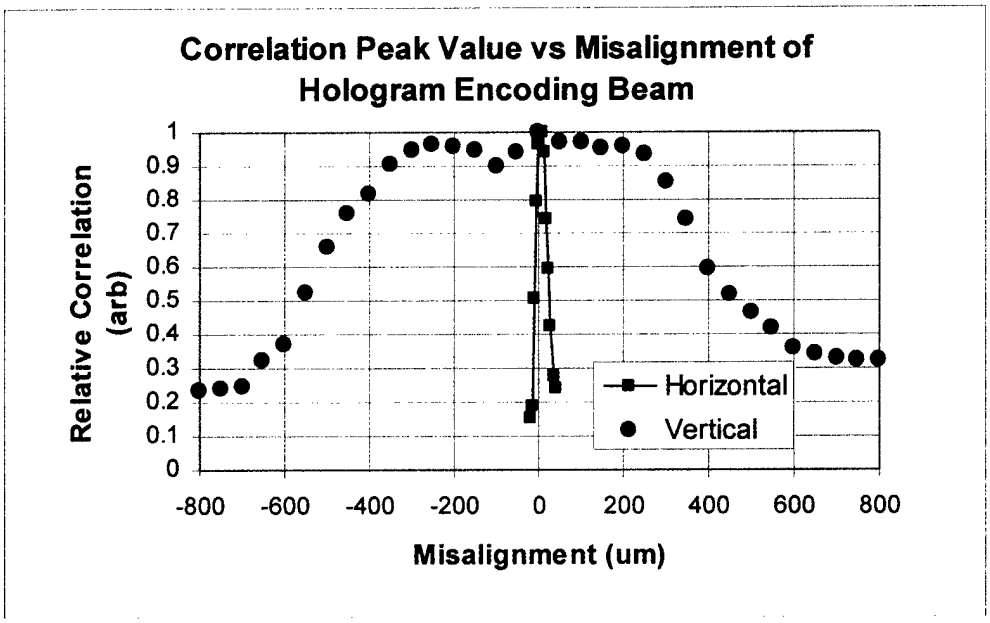


Figure 22. Variation of the correlation peaks as the Card Hologram is moved to different horizontal and vertical positions relative to a one-dimensional decoding reconstruction wavefront.

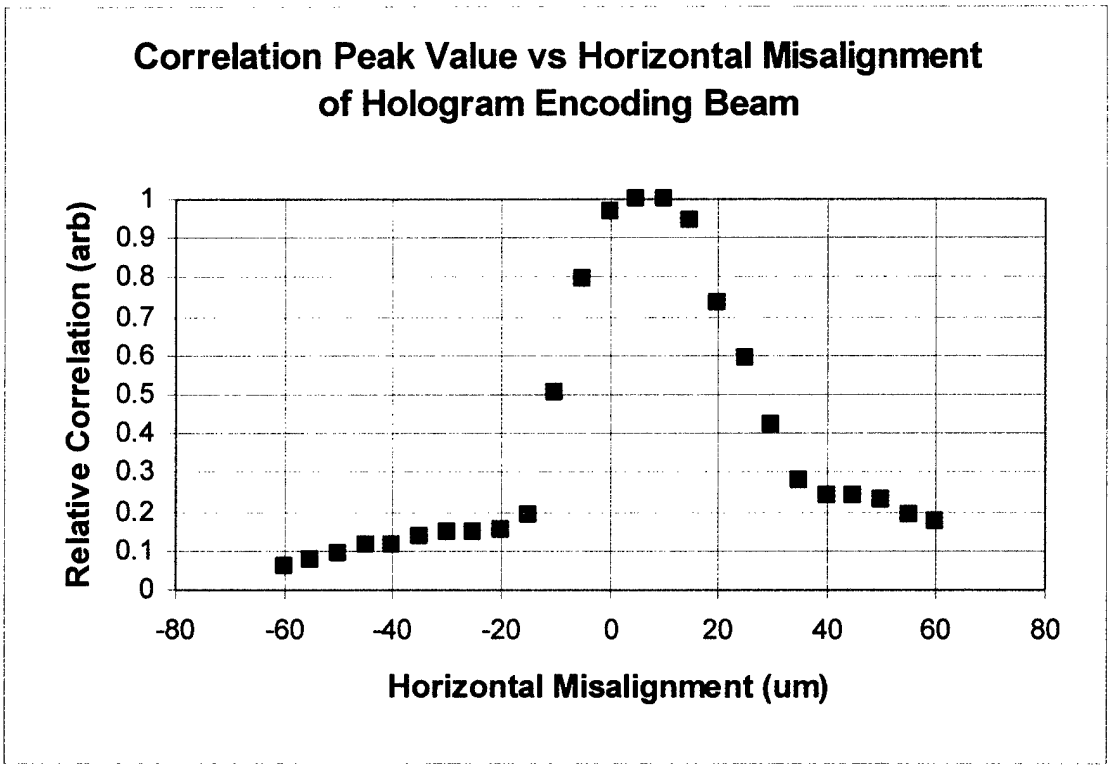


Figure 23. Variation of the correlation peaks as the Card Hologram is moved to different horizontal positions relative to a one-dimensional decoding reconstruction wavefront.

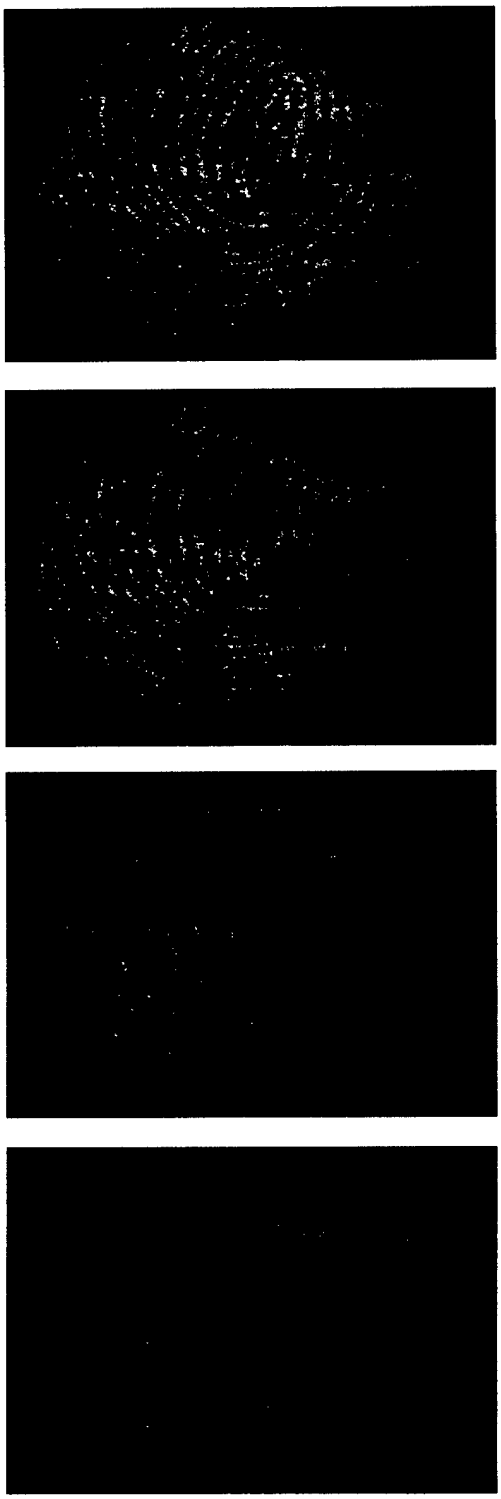
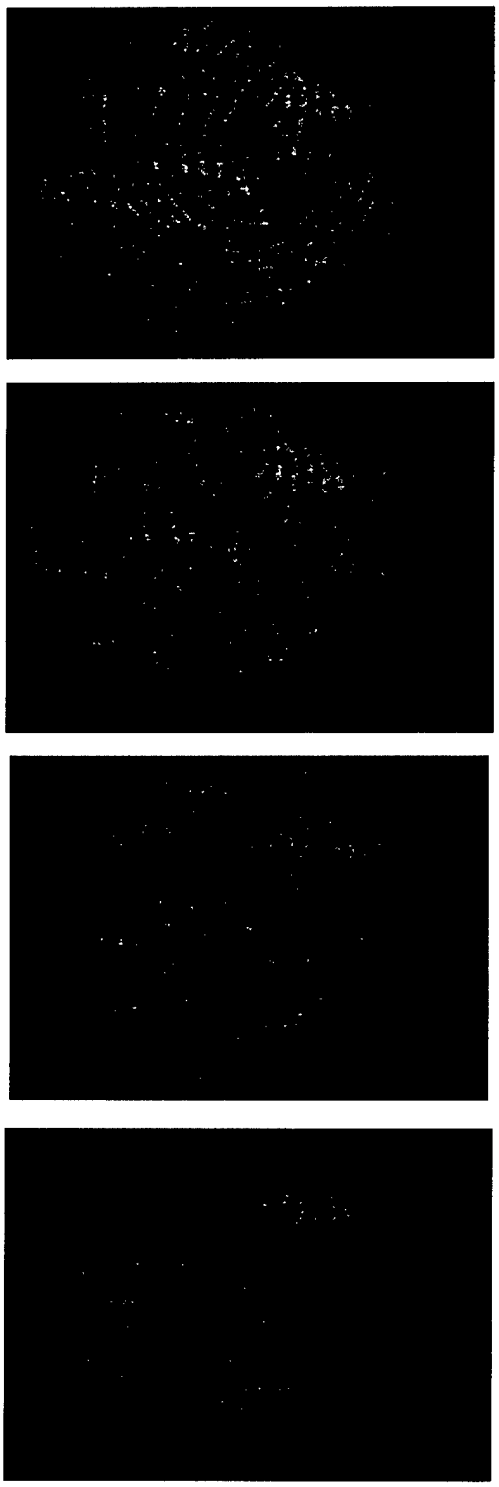


Figure 24. Image of fingerprint contained in Card Hologram as the coded reference beam is moved horizontally with respect to the hologram.



Reconstruction Beam Location (um)

(0,0)

(0,200)

(0,400)

(0,1000)

Figure 25. Image of fingerprint contained in Card Hologram as the coded reference beam is moved vertically with respect to the hologram.

Hologram Selectivity as a Function of Speckle Size

In order to test the selectivity and security of the Card Hologram using random beam encoding, volume holograms were also made using a thicker hologram material, Fe doped (0.05%) $LiNb0_3$ crystals. Although not the primary candidate for the final card, there are a number of reasons why this material is a convenient media for examining the security properties of thick holograms for the Air Force application. First, it is a real-time material that requires absolutely no processing and can be used to record multiple holograms that remain extremely stable under low intensity retrieval beams from the same laser used during recording. Though very stable, the recorded holograms can also be subsequently erased, thus regenerating the material for a new set of recordings. The $Fe:LiNbO_3$ used in our tests also have the advantage that the diffraction efficiency is largely unaffected by the frequency of the recorded fringes, thus allowing considerable flexibility in the experimental geometry. MetroLaser has numerous samples available in-house of varying thickness, thus allowing us to examine the effect of this parameter on the recording process and security of holograms made using random encoding. Finally, MetroLaser personnel have significant in-house experience regarding the properties and use of this material.

$LiNb0_3$ exhibits a strong refraction index modulation in the visible and can be used to produce holograms with diffraction efficiencies of up to 75-80% for a sample thickness of 500 μm or more. The major mechanism responsible for hologram formation in this material is refraction index modulation through the electro-optical effect. However, several physical processes are known to be involved in formation of this electric field, such as spatial redistribution of the photo-induced and trapped electrons by their diffusion or mobility in an externally applied field, photovoltaic or pyroelectric fields. These physical processes contribute to a variety of temporal and spatial characteristics in hologram formation and to the material's high diffraction efficiency.

A speckle-encoded reference beam was used to record holograms in thick (2 mm to 10 mm) $Fe:LiNbO_3$ crystals. The setup used is shown in **Figure 26**. In order to limit the number of variables, experimentation was conducted using circular speckles formed by a symmetric diffuser with an average size $<\sigma>$. In these experiments, $<\sigma>$ was varied from 50 μm to 100 μm by changing the size of the illumination spot on the diffuser. An expanded image of the speckles recorded by the hologram is shown in **Figure 27**.

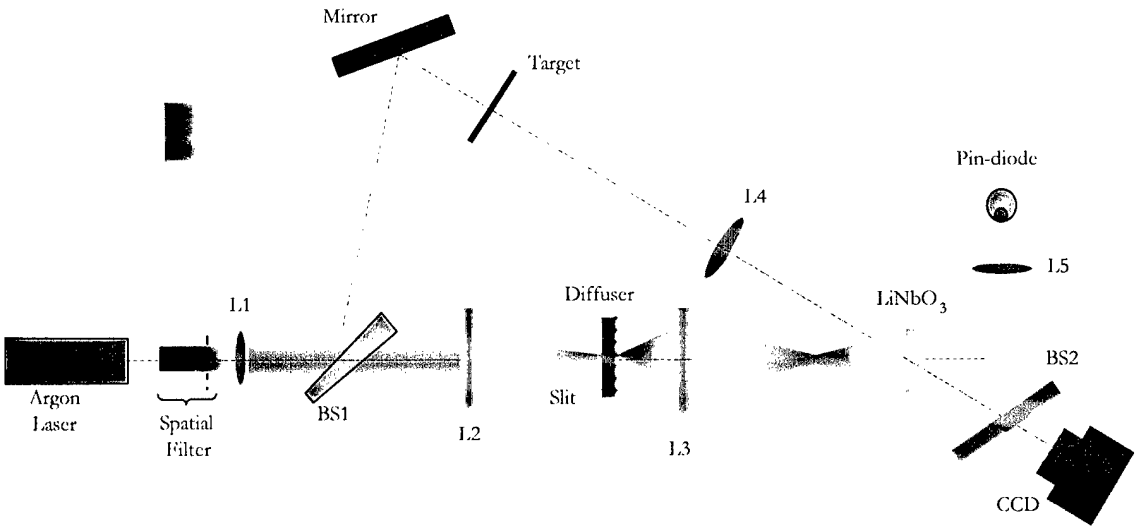


Figure 26. Test setup used to evaluate thick hologram material for making the Card Hologram using an elongated speckle pattern as the reference beam.

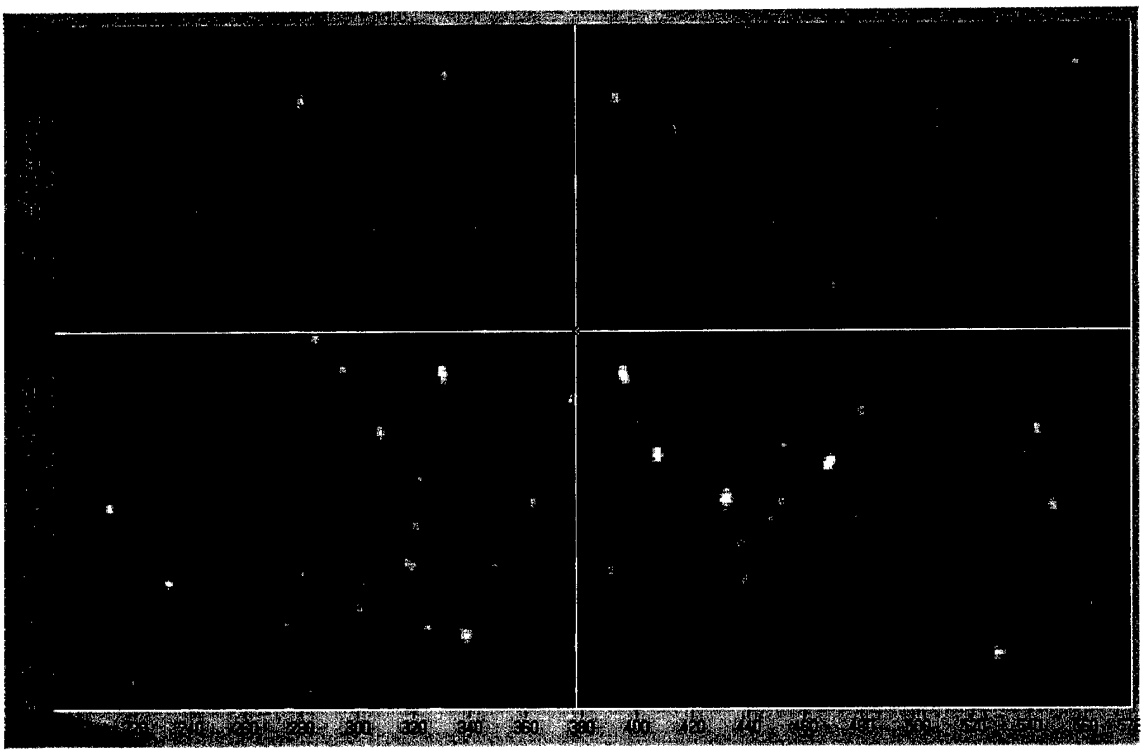


Figure 27. CCD image of the speckle wavefront used to encode the Card Hologram. Units are in pixels, with each pixel being a little under 10 μm in size. The average speckle size is approximately 50 μm both horizontally and vertically.

The speckle-encoded reference beam was combined with a collimated object beam containing a resolution target that was re-imaged onto a CCD array using the lens, L4. During reconstruction, the beamsplitter BS2 was used to direct the collimated object beam to lens, L5, which focused the energy onto a pin diode. The energy focused onto the pin diode was used to evaluate the relative efficiency of the hologram made using the speckle encoded reference wave.

The sensitivity of the hologram to alignment was evaluated by recording changes in the diffracted energy reflected by BS2 and focused onto the pin diode by L5. The results are shown in **Figure 28** for misalignment in the horizontal and vertical directions. Although the speckle pattern is very isotropic in both the **X** and **Y** directions, **Figure 28** indicates that speckle selectivity was, however, strongly asymmetric. For estimated average speckle size $\langle\sigma\rangle \approx 50$ μm the diffraction efficiency dropped to zero at about ± 25 μm shift in y (direction normal to the hologram dispersion plane); however, the shift selectivity in the dispersion plane (x direction) was more than twice as strong at only ± 10 μm. The corresponding reconstructed images of the resolution chart are shown in **Figure 29** for various amounts of horizontal displacement.

Very similar results were observed for holograms recorded with $\langle\sigma\rangle \approx 100$ μm (see **Figure 30**). The shift selectivity in the dispersion plane in this case was approximately ±20 μm, while the shift in the tangential plane was about ± 60 μm (close to the estimated speckle size). This asymmetric effect was also observed to depend on the crystal thickness, T. Increases in T resulted in a proportional increase in the speckle selectivity in the dispersion plane and had little effect on the selectivity in the tangential direction.

While not expected, the observed asymmetry in shift selectivity of the volume hologram recorded in this case may actually prove useful for our purposes, since such asymmetric selectivity is the ultimate goal in the Card Hologram.

The explanation of the asymmetric response is found when it is realized that there are actually two effects influencing the horizontal (x) component of the shift selectivity. Referring to L3 in **Figure 26**, each speckle in the hologram may be considered as consisting of a spherical wave that envelopes the speckle. It is well known that a spherical reference wave can be used to produce a volume hologram that is position sensitive at reconstruction. The shift selectivity is the result of the sensitivity of the diffracted wave to the spatial distribution of the k-vectors in the read-out spherical wave and angular selectivity for each of spatial components in the reconstruction beam. Once the hologram is displaced in the dispersion plane, the propagation direction of the corresponding k-vectors is not strongly affected by the K-vector of the formed grating. Therefore, the shift selectivity (ΔX_{SPH}) in this direction can be estimated as displacement at which the exact Bragg condition for the particular component is broken and can be expressed as

$$\Delta_{X_{SPH}} = \frac{\lambda z}{T \sin\theta},$$

where z is the distance between the focal point of the lens used to generate the spherical reference beam, hologram θ is the recording angle, and λ is the reconstruction wavelength. For our experimental conditions ($T \approx 2.8$ mm; $\lambda = 0.514$ μm, $\theta \approx 45^{\circ}$ and $z = 10$ cm), the estimated value of ΔX_{SPH} is 25 μm, which is in close agreement with experimental results for spherical wave selectivity.

In our case, the selectivity along the x-axis is the combined effect of this spherical wave selectivity and the spatial speckle decorrelation. The joint action of these two factors determines the actual shape of shift selectivity in this direction. A typical example of this is shown in **Figure 31**, where three curves illustrate different sensitivities of the diffracted beam intensity relative to the lateral shift in the dispersion plane.

The situation is less complicated for spatial shift in the tangential direction (Y-shift). In this case, the speckle spatial decorrelation is the only effect that leads to a decrease of the diffracted beam intensity, as there is almost no sensitivity for a spherical wave component (there is a very small value of grating K-vector in this plane). Therefore, shift selectivity in the tangential direction is truly speckle-based and corresponds to average speckle size in this direction for all experiments.

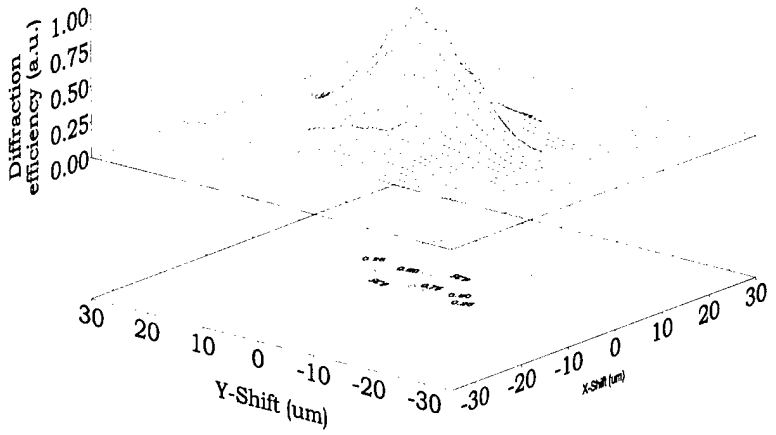
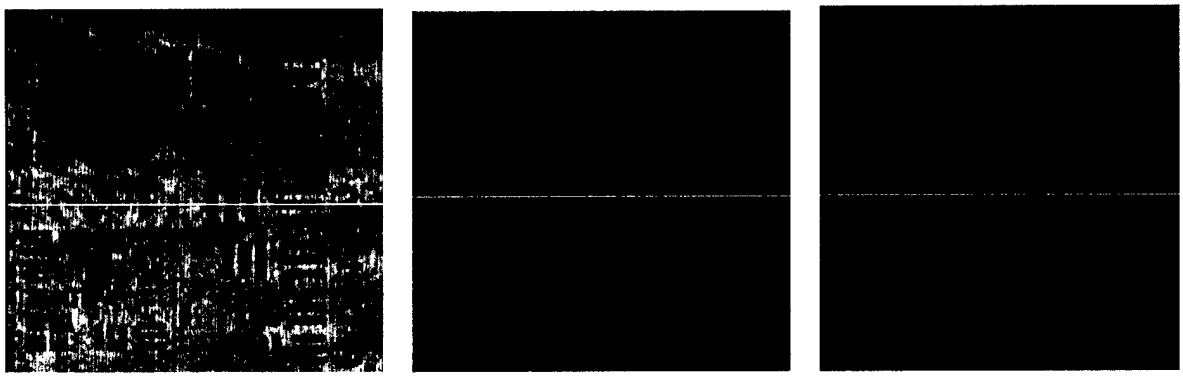


Figure 28. Total diffracted energy by the speckle encoded Card Hologram as a function of misalignment of the decoding speckle reconstruction beam in the horizontal and vertical directions. Average speckle size was approximately 50 μm. Results show that the selectivity is strongly asymmetric (50 μm in the y-direction vs. 20 μm in the x-direction).



(0,0) **(10,0)** **(15,0)**

Figure 29. Resolution target image for various amounts of horizontal misalignment of a $LiNbO_3$ hologram recorded using a 50 μm random speckle reference beam. The hologram location is indicated below each image.

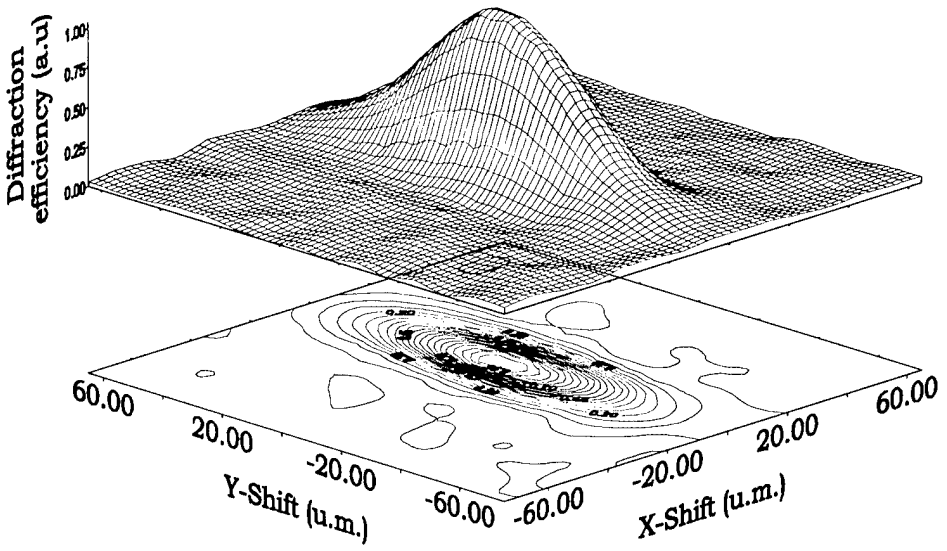


Figure 30. Total diffracted energy by the speckle encoded Card Hologram as a function of misalignment of the decoding speckle reconstruction beam in the horizontal and vertical directions. Average speckle size was approximately 100 μm. Results show that the selectivity is strongly asymmetric (120 μm in the y-direction vs. 40 μm in the x-direction).

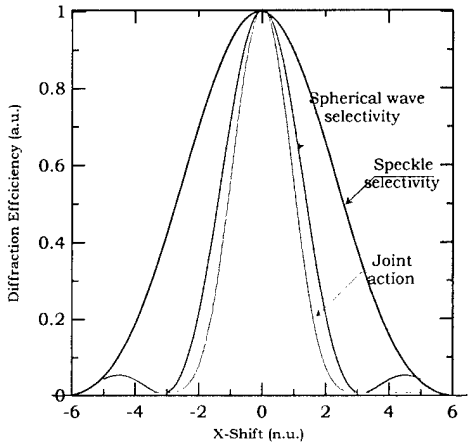
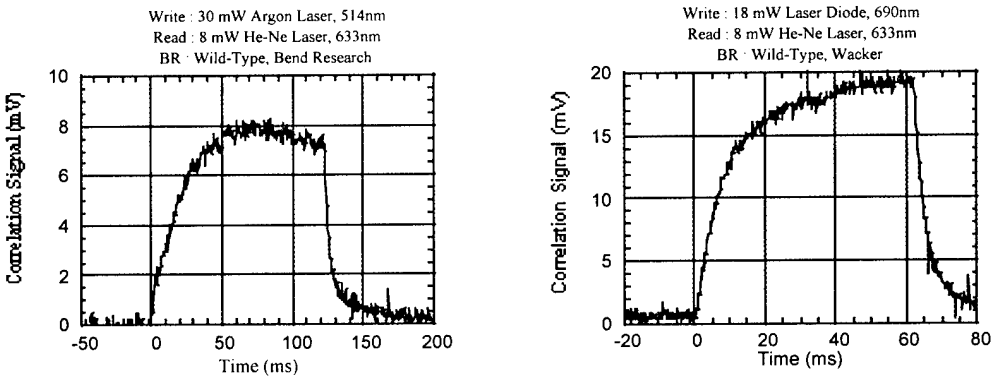


Figure 31. Calculated dependencies of the diffraction efficiency for spherical wave shift selectivity, speckle selectivity, and joint actions of the two mechanisms at the hologram shift in the dispersion plane.

Development of a Compact Optical Correlator Using Laser Diodes

A major step in the development of a commercial BR-based optical correlator is to replace the large, expensive Argon-ion lasers with compact, inexpensive laser diodes; however, laser diodes are presently available only at wavelengths above 630 nm, and not at the Argon-ion wavelength of 514 nm. Several tests were performed to measure the correlator performance with a 690 nm laser diode for the writing beams. Surprisingly, the system showed better overall performance with the laser diodes than with the Argon laser. **Figure 32** shows the time response of the correlation signal for two different write beams: a) 18 mW at 690 nm; and b) 60 mW at 514 nm. Both cases used the same Helium-Neon laser for the reading beam. A shutter (rise/fall time < 1 ms, open for 60 ms) was used in the path of the writing beams. Despite the lower power of the diode laser, the correlation signal was much higher with the writing beams at 690 nm than at 514 nm. Also, the rise and fall times of the correlation signal appeared to be slightly faster with the laser diode. These results were somewhat unexpected because the absorption of the BR ground state is much higher at 514 nm than at 690 nm. These experimental results were produced with BR films produced by both Bend Research, Inc. and Wacker, Inc., which indicates that it may be a general property of "wild-type" BR, rather than a unique feature of BR produced by a particular manufacturer.



a) b)

Figure 32. Time response figure of the correlation signal for: a) 514 nm write beams; b) 690 nm write beams. (The shutter was open for 120 ms for (a), and 60 ms for (b)).

The use of laser diodes means that it may be possible to make an all-optical fingerprint correlator that is fairly compact and inexpensive. The system would require only two laser diodes, a lens, a beamsplitter, a detector, and the BR film or SLM. There are several possibilities for the inputting of the images into the system, including photographic film, transparencies, and an electrically-addressed SLM. For fingerprint detection, a person could place their thumb on a prism, and the laser could pick up the fingerprint pattern from the frustrated total internal reflection of the prism. This image could be compared to an image stored onto an encoded reference card, or to an image stored on a computer and generated by an electrically addressed SLM.

Recently, a great deal of attention has been paid to JTC-based, real-time optical processors for fingerprint identification. Several research groups, including Thomson-CSF, the Jet Propulsion Laboratory, and AT&T Bell Labs, have performed system studies on these processors.[5] The Thomson-CSF group has developed a compact fingerprint identification correlator, employing a diode-pumped doubled Nd:YAG laser as the pump light source, and a photorefractive crystal, bismuth silicon oxide (BSO), as the

real-time holographic recording element. Our present experimental results with BR demonstrate several outstanding improvements to the Thomson-CSF system:

1. All Laser-diode operation. Based on the recently observed high diffraction efficiency with 690 nm pump light, an all laser diode-based correlator can be constructed. This greatly reduces the size, cost, and power requirements of the system.
2. Use of a third laser beam for "high-pass" filtering greatly improves the discrimination of the system.
3. Use of BR in place of the photorefractive crystal BSO. The BR reduces the cost and simplifies the alignment of the system.

Characterization of BR as a Correlator

Experimentation was performed to characterize the non-linearities of the photochromic BR material to investigate the use of this material to replace the CCD array, thus resulting in an all-optical JTC. Two collimated beams, 3 mm in diameter and separated by 38 mm, were focused onto the BR material using a diode laser write beam ($f = 200$ mm; $\lambda = 695$ nm). A HeNe laser was used to "read" the grating after a certain exposure time by the write beam. The voltage induced in a photodetector by diffracted power from the grating recorded in the BR was then recorded. **Figure 33** shows the relative amount of power diffracted for various exposure times for two different beam intensities. For the intensity levels used, a type of reciprocity failure is seen to occur, in that for a given amount of total exposure energy (power x time), the amount of diffraction signal differs, depending on the amount of power in the write beam

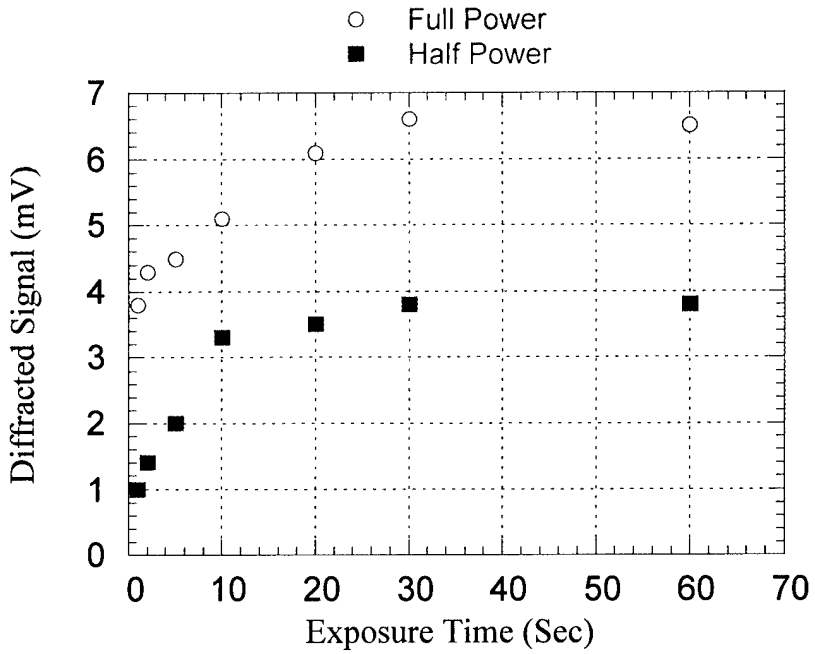


Figure 33. Experimental results showing the diffracted signal as a function of exposure time. Experiments were conducted at two different laser intensities.

SYSTEM DEVELOPMENT

Various issues and features related to the Phase II prototype security system are reviewed in the following sections. Most of the following material is summarized from material contained in the various technical quarterly reports submitted to the Air Force during the course of the Phase II program.

Format of the Data Contained in the Holographic ID Card

During the course of the Phase II program, three options were examined for the content of the Key/Card Holograms.

In the first option, a random phase mask alone is released by the Key/Card Hologram pair. This phase mask is compared to the reference mask in the reader as a means of authenticating the item to which the hologram is attached. Example applications include an entry or computer key and an authentication marker for a document or product.

A second option is to also attach an amplitude (or phase) image of some sort that either further verifies the authenticity of the object or links the object (card) to the person presenting it. The attached image in this case is some type of biometric information. A JTC or some other type of correlator is used to verify the authenticity of the phase mask contained by the hologram. If a JTC is used, it might also be the best choice for correlation of the amplitude image contained in the hologram, depending on the complexity of this image. This option can be used where a visual image would be more meaningful to a human inspector than an invisible, random phase mask.

In the third option, the hologram contains image information that is digital in nature and is read directly by a CCD camera. Technically, this is similar to the previous option except that the digital format is better suited for interpretation by a computer. In the case of an ID card containing fingerprint information, rather than store the image of a fingerprint, this information is reduced to a smaller number of bytes that uniquely characterize the fingerprint. This digitized information can be stored on the hologram through the use of a SLM in which each pixel or set of pixels represents one bit of the digital code. Since the data is in a digital format, a JTC is not required to perform the fingerprint correlation. The digitized fingerprint information can either be compared to a database (located remotely or inside the reader) or to a live image of the fingerprint that is reduced to a binary code using the same algorithm used to reduce the holographically stored fingerprint.

One advantage of this last approach is a psychological one. People tend to feel apprehensive about jeopardizing the anonymity of their biometric information by storing it on a card that could be lost or stolen (PIN's can be changed, fingerprints cannot). Whether real or imaged, there is the perception that a digital representation of this information is less revealing than the actual biometric information itself. In the area of biometrics, this approach also has the advantage of greater flexibility. For instance, the information on the card could just as easily be a digital representation of a voice print or key stroke style that could not be recorded as a direct image. A summary of these three options is given in **Table 1.**

Table 1

Type of Amplitude Information	None	Image	Digitized Image
Features	Authenticates the object to which it is attached. Phase mask authenticated using a JTC to correlate to a reference mask in the reader.	Authenticates object and contains an image that is associated to the object or owner. The phase mask is verified using a JTC, while the image is verified either visually, with a JTC, or some other correlating algorithm.	Authenticates object and contains a digital image regarding the object or owner. Successful reconstruction of the digital image authenticates the hologram, while the attached information authenticates the object or owner.
Applications	Documents *(green card, passport, bonds, official papers).* Credit Card. Currency. Key *(entry, computer, network/internet).*	Documents *(green card, passport, bonds, official papers).* Credit Card. Products *(software, electronics, OEM, retail).* Art objects. Currency. Tokens. Key *(entry, computer, network/internet).* Biometrics.	Documents *(green card, passport, bonds, official papers).* Credit Card. Products *(software, electronics, OEM, retail).* Art objects. Currency. Tokens. Key *(entry, computer, network/internet).* Biometrics. Internet *(commerce, ID/authorization, encryption key storage).*
Competing Technologies	Holograms. Kinegrams. Variable inks.	Holograms. Photos with added security features.	Smart Card. LaserCard. Magnetic strip.
Advantages ***(compared to other amplitude information options)***	Content not obvious to forger. Simplest implementation. Easily verified by JTC.	Higher security than for simple phase mask. Contains more information than simple phase mask. Equally suited to human or machine inspection.	Information is more compact than images. Large data capacity *(multiplexed holograms).* Well suited for digital processing. Biometric information is perceived as more secure in case of loss or theft. Flexibility in types of biometric information contained. More robust to wear.
Disadvantages ***(compared to other amplitude information options)***	No information storage. Difficult to produce a JTC reader for larger or odd shaped products.	In JTC, phase code dominates correlation. Rotational alignment is critical in JTC. Inefficient format for storing digital information.	Information meaningless to human inspector. Logical applications compete with Smart Card technology. As compared to Smart Cards: - Not read/writeable. - Expensive reader. - More sensitive to wear?

Correlator Options

Depending on the content of the encrypted Card Hologram, a number of approaches are available for validating the authenticity of the hologram to be used in the ID card validation system. The validation system has the following key elements:

1. A volume hologram to secure the content of the card, which is produced using a complex encoding beam (the Card Hologram).
2. A random phase mask and biometric information, released by the Card Hologram when illuminated by the proper decoding reconstruction beam.
3. A reference phase mask for comparison to the phase mask encrypted in the ID card.
4. A live biometric for comparison to the biometric information encrypted in the ID card.
5. A method of validating the authenticity of the card (correlation between the reference and card phase masks).
6. A method of validating the authenticity of the cardholder (correlation between the live biometrics and those stored on the ID card).

One method of achieving Elements 5 and 6 is through the use of a JTC. Two configurations of the JTC have been examined. The first is to perform an optical Fourier transform of the reference and card information using a lens, and then electronically calculate the correlation function using data from a CCD located in the Fourier plane of this lens. This method has been implemented by Physical Optics Corporation. To avoid duplication of effort, MetroLaser contacted POC to determine if they would be interested in supplying this part of the card evaluator for the MetroLaser reader. Despite repeated efforts to contact POC, we received no response as to their interest.

As an alternative, MetroLaser examined the possible use of an all-optical correlator by replacing the CCD with a photorefractive material such as Bacteriorhodopsin (BR). Using this approach, the interference between the reference and signal beams produce a grating that is illuminated by a low power read beam. The Fourier transform of the read beam is obtained by passing it through a lens to produce the correlation signal.

One problem with using the JTC when both the random phase mask and biometric signal are superimposed on top of one another is that it is difficult to perform separate correlations on each. Also, the use of a lens to perform the correlation does increase the size and complexity of the reader. This tradeoff is offset by the gain of shift invariance and the extreme speed with which a correlation can be made between two complex signals, such as the random phase mask used for security. For a less complex signal, such as two fingerprints, the advantage of the JTC over other methods of correlation becomes less compelling.

As we evaluated and compared the various validation means for the process in Element 5, we came to realize that the Card Hologram itself could be used to perform a correlation between the original (complex) reference wavefront used to record the hologram and the reconstruction wavefront contained in the reader. This would effectively replace the function of the JTC with a potentially much simpler and less expensive solution to the card validation task of Element 5. In this case, successfully reconstructing the object wavefront (random phase mask and/or biometric information) would be tantamount to validation of the card's authenticity.

This leaves the task of validating the biometric information (Element 6). This could be accomplished using either a JTC or some other correlation method. In the case of fingerprints, which have a relatively small amount of information as compared to other biometrics, a more direct comparison algorithm might be more suitable. Commercial products that interface with a PC currently exist that reduce a fingerprint to around 250 to 1000 bytes. This information could be converted to the required 2,000 to 8,000 binary

bits using an SLM. The resulting digitized image could then be recorded onto the Card Hologram and played back directly into a CCD array located in the reader. The resultant reader would consist only of a laser, the Key/Card Hologram and a CCD array. The simplicity of this system results from allowing the hologram itself to act as the correlator for verifying the authenticity of the Card Hologram.

A schematic of the reader, the approach ultimately chosen by MetroLaser for the Air Force system, is shown in **Figure 13**. In this approach, the biometric information on the Card Hologram is reduced to a binary code that is directly read by a CCD or CMOS detector array. This type of compressed format of the biometric information is used by a number of commercial fingerprint systems for use on PC's. The compressed fingerprint code is digitized and stored on the hologram during enrollment through the use of a spatial light modulator (SLM) in which each pixel or set of pixels represents one bit of the digitized code. During presentation, the digitized representation from the fingerprint reader used at the point of entry into a secured area is compared to the information stored in the encrypted Card Hologram. A number of robust algorithms currently exist commercially that are used with very high reliability to compare the two such binary codes in the presence of noise to determine if they were generated from the same fingerprint.

Fingerprint Reader

MetroLaser incorporated a fingerprint reader marketed by Saflink Corporation into the holographic card reader. The SAF/NT 2.0 is based on a solid-state fingerprint sensor produced by Veridicom, Inc., a spin-off of Lucent Technologies. One interesting feature of the Saflink approach is that it also incorporates digital representations of voice and face biometrics, along with the fingerprint information. Ultimately, the digitized information from all three biometrics could be stored on the Card Hologram and compared to the live versions upon presentation of the ID card. The incorporation of multiple types of biometrics, and in particular the use of voice data, is something that could not easily be handled using JTC.

The fingerprint reader comes with software that allows it to be installed into a desktop computer, enroll up to ten fingers for each authorized user, and later compare the enrolled fingerprints with a live presentation. The system can also be incorporated with computers using the Windows NT operating system to limit computer use to enrolled individuals, replacing the need for entering a password.

CMOS Detector

In an effort to reduce the cost of the final ID card reader, a CMOS detector array was selected and tested with the system developed for the Air Force. CMOS image sensors are specialized integrated circuits (ICs) that in recent years are being considered in many applications traditionally incorporating CCD technology.

The sensor core typically consists of an array of photodiodes which detect visible light. CMOS transistors co-located in each picture element (pixel) select, amplify, and transfer the photodiode signals. A CMOS imager, or imaging system, comprises the sensor core and various ancillary circuits. The latter further amplifies the signal, suppresses noise, processes the detected image, and translates the digitized data into the most optimum format for each application.

There are a number of characteristics of CMOS arrays that make them well suited for the Air Force application. First, they are considerably less expensive than CCD arrays. Due to their relatively simple structure, CMOS detectors result in a much smaller package than an equivalent CCD. Finally, CMOS arrays consume significantly less power, leading to longer battery life and/or smaller power supplies.

The main drawback to CMOS detectors has traditionally been image quality; however, for the version of the card reader shown in **Figure 13,** this is not a significant disadvantage. Also, the CMOS technology is advancing at such a rate that the image quality advantage of the CCD detectors is quickly diminishing.

For example, the primary source of noise in CMOS detectors is known as reset or kT/C noise: a time-varying voltage offset created when a capacitor is reset after having been read. The reset noise is inversely proportional to the capacitance and is the dominant read noise of a CCD (on the order of 100 or more electrons root mean square) unless off-chip correlated double sampling is used to suppress this noise. Recent work, however, has demonstrated that this noise can be significantly decreased using an active reset.[6]

A CMOS detector and engineering development kit was purchased from Smart Vision Products and was integrated into the card reader system. The initial performance appeared excellent. The CMOS detector was ultimately not used in the prototype card reader due failure on the part of the distributor to provide sufficient software access to necessary camera functions. Due to their low cost, however, a CMOS detector will ultimately provide the best solution.

Reading of SLM in Card Reader

The transfer of data from a hologram into a computer, microprocessor, or other electronic device requires that the information on the hologram be in a digital format. To accomplish this, a device such as a SLM is used to produce an image that takes the form of a two-dimensional array of pixels that can be individually addressed to vary the attenuation of an input laser beam or wavefront. By setting an individual pixel for either maximum or minimum attenuation, each array element is used to represent one binary bit of a digital code. The SLM can also be used to provide gray scale variations in order to allow each array element to represent more than one bit of information. The data capacity of an individual pixel is $\log_2(n)$, where n is the number of gray scale levels.

To read the digitized image stored on the hologram, a detector array, such as a CCD or CMOS, is used to read the optical information. In order to reliably read the information, the array image from the SLM or hologram must be aligned spatially in three dimensions. That is to say, the image of the SLM array must be overlaid on top of the detector array and the image must be positioned so that each SLM pixel is aligned to a corresponding pixel on the detector array.

To develop and characterize the performance of this optical method of writing and reading digitized information, an SLM and detector array were configured in the holographic card reader as illustrated in **Figure 34**. A digitized code was generated by the SLM that was imaged onto the detector array. An iris was placed in the focal plane of the lens to filter the unwanted diffraction orders produced by the periodic spacing of the SLM pixels. Since a hologram creates additional noise and image distortions, the setup in **Figure 34** was used to isolate and solve technical issues unrelated to the hologram such as alignment between the SLM image and detector array, detector and SLM noise/dropout, and software algorithms used to write and read the optical format.

The configuration shown in **Figure 34** was utilized in the card reader and card writer developed for the Air Force. In the card writer, a hologram was located about an inch in front of the location of the detector array in **Figure 34**. In the reader, this digital image was then projected onto the detector array. The hologram, therefore, effectively replaced the SLM, lens, and aperture in the card reader.

Software algorithms were developed to write a digitized code to the SLM and to read the imaged code back when displayed on the detector array. The format for the data that is written to the SLM is shown in **Figure 35**. The SLM pixels are represented by smaller grid elements shown inside the array's active area. The four dark boxes in the four corners of the array are pixels that contain no data, but are used for alignment purposes and are set to maximum attenuation. The corner for each of these four boxes that is closest to the center of the array are at known locations within the array and can thus be used during reading to set the scale and orientation of the reader pixels relative to those of the SLM. The pixels

located in the shaded area in the center of that SLM contain the digitized data that is read by the detector array and will eventually be recorded onto a hologram.

The projection of the SLM image onto the detector array is shown in **Figure 36**. The active area of the detector array is shown as slightly smaller than that of the SLM and with a slight amount of relative tilt. The four dark corners of the SLM are contained within the detector area and are used to establish horizontal and vertical scaling and to correct for the tilt between the two arrays.

Tests were conducted in which known, repeated patterns were generated over the entire SLM. The detector location and limiting aperture were adjusted to produce the best SLM image onto a CMOS detector array. The pixel pitch of the CMOS detector was 12 μm x 12 μm, while that of the SLM was approximately 23 μm x 23 μm. The imaging optics were adjusted to produce a magnification of 1 SLM pixel to 2 CMOS pixels. Tests were also conducted using a CCD detector array with a pixel pitch of 8.4 μm x 9.8 μm in place of the CMOS. The magnification in this case was approximately 1 SLM pixel to 2.25 CCD pixels in one axis and 1 SLM pixel to 2.6 CCD pixels in the other.

Once the SLM and detector were properly aligned, tests were conducted in which the data area contained a known, random code and was projected onto either the CMOS or CCD detectors. Each bit of the code was represented by a value of either no attenuation or full attenuation over an area of the SLM of 2 pixels x 2 pixels. Each data "bit", therefore, occupied approximately 4 pixels x 4 pixels on the CMOS detector and 4.5 pixels by 5.2 pixels on the CCD detector. The exact scaling was calculated during each test by the program based on the location of the four dark corners generated by the SLM for alignment and shown in **Figure 35**. The relatively large SLM area and binary gray scale were used in order to make the alignment process as simple as possible in the initial prototype system. In future systems, the number of SLM and detector pixels representing a "data bit" will be decreased to increase the data density. The use of gray scale interpretation of the pixel value also can serve as a method of increasing the amount of data contained in the wavefront.

To test the reliability of the system using the initial test parameters, a series of known, random codes were written to the SLM and read back by the detector. For each test, the code read by the detector was converted back into a digital value and compared to the original code written to the SLM. Experiments in which several hundred codes were written and read were conducted and the location of bits that contained errors was tracked.

The system was found to be generally reliable; however, some data bits proved to be considerably more prone to errors than the rest. The system also seems to be extremely sensitive to slight changes in alignment. Possible error sources included:

1. Bad detector pixels.
2. Bad SLM pixels.
3. Uneven illumination across the wavefront into the SLM.
4. Problems in the method of determining threshold.
5. Problems in the algorithms to determine scale and/or relative tilt between the SLM and detector array.
6. Problems in the algorithms to determine the value of the data bit represented by a set of camera pixels.

To correct for occasional errors in the reading of the SLM pixels, a Reed Solomon routine was developed that is able to correct up to 32 errors in each group of 223 bytes of data.

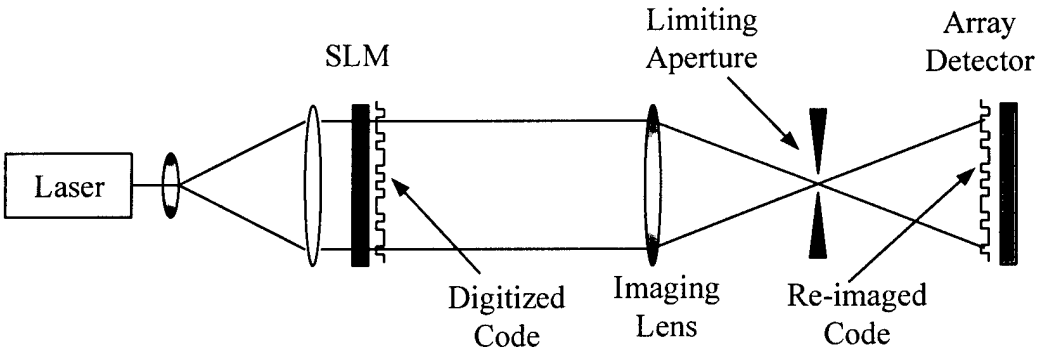


Figure 34. Experimental setup to develop and characterize the performance of writing and reading optically digitized information.

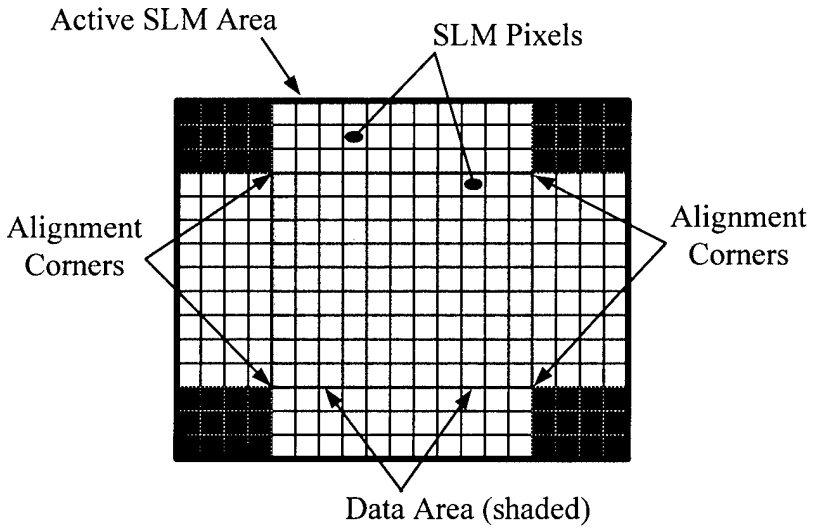


Figure 35. Format of the SLM data.

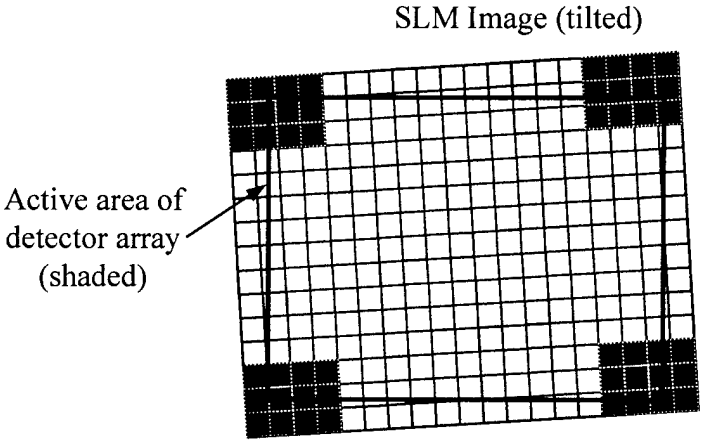


Figure 36. Reading of the optically digitized data onto a detector array.

COMMERCIALIZATION INVESTIGATIONS

Machine Readable Holographic Token

Various potential spin-off applications of the technology developed for the U.S. Air Force developed during the Phase II program were investigated during the course of the Phase II program. One such application involved the gaming industry where there exists a serious counterfeit problem of tokens used in casino slot machines. Various counter measures have been tried to combat the problem, but with rather limited success. Capra Technologies of Tampa, FL invited MetroLaser to join a consortium of companies to address this problem. Capra's longer-term goal was use technology developed for this application to produce products for the healthcare industry. There is a desire in the healthcare industry to develop a database system in which each patient carries a card containing confidential information that would need to be protected in the event the card were lost or stolen.

Capra was initially interested in the technology being developed for the Air Force, but we quickly determined that a number of features and technical challenges specific to their application precluded the immediate use of the "Key/Card" technology. Instead, we investigated an alternate approach based on more traditional embossed holography technology that will incorporate the use of multiple detectors in a reader to determine the authenticity of the token.

As a preliminary demonstration, Capra partially funded an effort to produce a prototype token reader/comparator for the gaming industry. The working prototype reader and holographic tokens were designed, constructed, and demonstrated to representatives from Capra and some of their key vendors.

After the demonstration, MetroLaser investigated the possibility of producing several thousand holograms and a number of readers in order to conduct field-testing of the system. We also talked with key personnel at Old Philadelphia Mint, a token manufacturer for the gaming industry located in Philadelphia, about producing readers to be used in conjunction with the token holograms. Old Philadelphia Mint was to mount the holograms to their gaming tokens. An order for several million holograms was anticipated if the first field system proved a success.

As a result of the business potential, we also sought patent protection on the axisymmetric hologram technology incorporated into the first demonstration token reader. With this reader, each token can be validated in an automated fashion, regardless of the rotational orientation of the token in the machine reader. As a way of contributing to the development and protection of this technology, Capra signed an agreement in which they would pay for the legal costs involved in the submission of the patent application.

We continued to talk with Capra Technologies about the development of a security token for use in the gaming and healthcare industries that would employ the technology being developed for the current project. We have also done some preliminary estimates of the cost of producing such holograms in quantities of over 1,000,000. The ring hologram originally conceived for this application would cost about 2 to 3¢ each. If a smaller hologram can be used in the center of the token, then the unit cost will be considerably less than 1¢ each for runs in excess of 1,000,000.

Dr. Cecil Hess, president of MetroLaser, met with personnel from Capra Technologies, Green Duck Incorporated (one of the largest manufacturers of tokens in the world), and Money Control, an international producer of automated coin readers. The discussions concerned potential plans to incorporate holographic security into gaming and other tokens. Green Duck expressed an interest in the development of a holographically secured token for their customers. The purpose of the meeting was to introduce them to the approach being taken by Capra to meet this requirement. After the meeting, a tour of the Green Duck minting facility was made.

While we are still pursuing the potential commercial application, the potential use in the gaming industry appears to be less compelling than initially anticipated. Two factors have resulted in this conclusion. First, the manufacture of tokens in the gaming industry is extremely competitive. While there is a strong interest in addressing the current fraud problem, there are also small profit margins involved in the sale of tokens. Fractions of a cent increase in the cost of a token must demonstrate a clear advantage over the competition before it will be attractive to customers. It appears that the cost of adding a hologram to the token would be on the order of 1 to 3 cents per token, which makes it very difficult to compete. A second factor involves a decrease in the token industry itself as it relates to gaming. The industry is quickly changing from the use of tokens to a system involving the using some type of electronic debiting.

Internet Application of Key/Card Technology

Another area of commercialization involving a more direct application of the technology developed for the Air Force involves the security of Internet transactions. Because this is a much broader application than originally proposed, the successful application of our technology into this arena would be of much greater value than that originally envisioned, both in the governmental and private sectors.

The use of the Internet in business-to-business transactions allows both government and industry to carry out contractual and purchasing functions in an extremely efficient manner. The realization of such an ambitious use of the Internet, however, makes extremely high demands in the areas of secure methods of transfer over public systems and positive identification of the user. These are exactly the strengths of the Key/Card technology being developed under this contract.

The use of electronic Smart Cards is currently being proposed as the main solution to this problem, with companies such as American Express testing consumer demand for such Internet security through the introduction of its electronic "Blue Card":

http://ctst.expoexchange.com/Content/conferenceandevents/frameset.asp

However, the exponential growth in the business-to-business (B2B) commerce and the use of digital signatures in creating legally binding transactions over the Internet have led to extremely high demands in the areas of secure transmission and positive identification. MetroLaser's Key/Card technology could potentially offer a greater level of security to an industry that is still young enough to entertain the incorporation of leading edge technologies such as ours. The security enhancements afforded by our Key/Card technology into an Internet security system would be extremely valuable by removing critical roadblocks in the development of a PKI (Public Key Infrastructure) system.

To help us evaluate the needs of this market and the potential application of the Key/Card technology, we produced both a consumer and a commercial survey. Each survey was set up on a MetroLaser web page and a link to these pages was attached to emails requesting the participation of the prospective respondents. The consumer survey was sent to people on email lists of various MetroLaser personnel. The commercial survey was sent primarily to a list of project managers involved in a program to incorporate Smart Card technology within all branches of the government (http://smart.gov/section04c.cfm).

The purpose of the consumer survey was to assess the public's understanding of Internet security and their perception regarding the use of biometrics as a means of identification during Internet transactions. The results indicated that about 50% of the respondents were unwilling to turn their fingerprints over to an e-business under any circumstance, while another 30% would do so only for sensitive transactions. This distrust from the general public indicates a need for guarding biometric information from inclusion on centralized databases. The MetroLaser security card could achieve such privacy needs by using a local database (the ID Card), which is in possession of the user only, as a means to confirm the biometric

identity of the cardholder. A match between the user's fingerprint and the fingerprint stored on the card would result, for instance, in the release of a Private Key used to encrypt a message and confirm the identity of the cardholder. In this case, the vendor never receives the fingerprint information directly, but simply an encrypted message that can only be made with the cardholder's Private Key. The security of the system is dependent on the fact that the fingerprint and the encryption key stored on the card can only be released by the cardholder's own fingerprint.

The commercial survey was designed to obtain the opinion of people involved in the Internet security industry regarding the adequacy of electronic Smart Cards to meet Internet security needs, and to determine if there are requirements that could be better met using an optical approach, which the MetroLaser technology incorporates, to increase both security and data capacity. The results of the commercial survey are shown in **Table 2**.

The response to Questions 3, 6, and 7 indicate that there is clearly a need for more security in government Internet transactions than is currently provided using the current encryption key + password system. Only 35% of the respondents agreed that this system provides sufficient security, while 43% said that it was clearly inadequate. Question 4 indicates that the addition of an electronic Smart Card increases confidence (49% responding yes), but half the respondents still indicated that they either believed this system would provide adequate security or they were unsure. The addition of biometrics clearly increased the confidence level for most respondents (68% responding yes).

Table 2: Results from Commercial Survey regarding Internet security.

Q1. In what sector is your organization?

Banking	E-retail	Government	Security	Other
0%	0%	92%	2%	6%

Q2. In what Internet transactions does your organization (or customers) require secure transmissions and/or positive identification?

Consumer Purchases	E-commerce	E-mail	Other
23%	62%	60%	38%

Q3. For these transactions, is PKI (encrypt + password) sufficiently secure?

Yes	No	Not Sure	No Opinion	N/A
35%	43%	20%	2%	0%

Q4. Does the addition of an electronic Smart Card to the PKI provide sufficient security?

Yes	No	Not Sure	No Opinion	N/A
49%	24%	27%	0%	0%

Q5. Does the addition of biometrics to the PKI provide sufficient security?

Yes	No	Not Sure	No Opinion	N/A
68%	10%	20%	0%	2%

Q6. How many of your users have significant security?

Majority	About Half	Minority	Don't Know
30%	10%	28%	32%

Q7. What means does your organization use to secure Internet transactions?

PIN/Password	Smart Card	Other Type Card	Biometrics	Other
90%	22%	2%	6%	18%

Q8. If your organization uses some ID and/or data card, what are the current applications?

Internet	Local Network	Medical Records	Transport	Access Control	Other	N/A
32%	30%	9%	18%	61%	11%	20%

Q9. If applicable, what is the data storage capacity of your current card in KBytes?

2	4	8	16	32		
7%	7%	27%	27%	27%		

Q10. What data capacity would an ideal card have for your application in Kbytes?

8	10	16	32	64	120	1024
7%	4%	7%	37%	37%	4%	4%

Q11. Using the following scale, rate the following attributes of an ideal card for your applications.

	Extremely Important	Moderately Important	Minor Importance	Not Important
Card Security	86%	24%	2%	
Data Security	76%	40%	2%	
Large Storage	14%	66%	16%	4%
Low Cost	62%	30%	8%	
Utilize Fingerprint Instead of Password	30%	38%	16%	16%

Q12. What price would your organization pay for an ideal card system?

Card:

<$0.50	$0.50	$1.00	$3.00	$5.00	>$5.00
7%	0%	28%	19%	21%	28%

Reader:

<$25	$25	$50	$100	$200	>$200
26%	26%	16%	23%	0%	9%

Q13. What types of problems would you anticipate if your organization implemented a new type of security card system?

Switching Cost	Contract Obligation w/Supplier	Lack of Acceptance by Users	Other
53%	30%	44%	28%

REFERENCES

[1] A.B. Coblijn, Proc. SPIE 1509, "Holographic Optical Security Systems", 14-15 March 1991, The Hague, Netherlands.

[2] B. Javidi, and J.L. Horner, "Optical Pattern Recognition for Validation and Security Verification," Journal of Optical Engineering, Vol. 33, No. 6 (June 1994).

[3] B. Javidi and J. Horner, "Optical pattern recognition for validation and security verification," Optical Engineering, Vol. 33, No. 6, pp. 1752-1755, (June 1994).

[4] B. Javidi, "Nonlinear Joint Power Spectrum Based Optical Correlation," Applied Optics, Vol. 28, No. 12, pp. 2358-2367 (June 15, 1989).

[5] D.M. Pepper, "The emergence of nonlinear optics in the factory," Optics and Photonics News, Vol. 8, pp. 32-40 (1997).

[6] B. Fowler, M. Godfrey, J. Balicki, & J. Canfield, "Low Noise Readout Using Active Reset for CMOS APS", SPIE Proceedings, V., 3965A (January 14, 2000).