Physical Optics Corporation

Optical Label and Reader to Prevent Counterfeiting

For many years, counterfeit products have flooded markets in the United States and overseas, cases of identity thefts are frequent, and breaches of security in controlled access areas vex airports and government offices. To address these problems, Physical Optics Corporation (POC), a California-based company, proposed in 1997 to develop a potentially foolproof method to verify and authenticate products and documents through their novel Optical Maximum Entropy Verification (OMEV) system.

Such an ambitious research project needed active financial support that POC could not provide and venture capitalists would not fund. So the company sought help from the Advanced Technology Program (ATP) in 1997, explaining that cost-shared ATP funding would expedite the development of this technology by at least three years and that its overall impact on the economy would be tremendous. The ATP-funded research project was launched in October 1997 and achieved all its goals within its three-year duration.

POC developed a laser-based system by which light rays would be beamed on a piece of polymer resin to randomly generate a two-dimensional array of patterns that acted as a master label. Product manufacturers would affix this label on each product, rather like an optical signature. The authenticity of each product would be established by comparing its label with the master label in a label reader. Because the intricate patterns on the OMEV labels would be randomly generated, POC claimed that the chances of these labels being forged were almost nil.

Based on the economic and security benefits of this system, heightened after the 9/11 tragedy, POC launched efforts to commercialize the technology; the resulting product is called "Optikey." In 2005, the company licensed the technology to a spin-off company and as of 2006, had received a favorable response from product manufacturers, the entertainment industry, government agencies, and credit card companies. The U.S. House Appropriations Committee allocated $1 million in 2005 and $1 million in 2006 to incorporate this system into existing security cards in the Departments of Defense and Homeland Security. POC also received three U.S. patents and one Taiwanese patent for its work and has made several technical presentations.

COMPOSITE PERFORMANCE SCORE
(based on a four star rating)
* * *

Research and data for Status Report 97-01-0244 were collected during March – June 2006.

POC Proposes Counterfeiting Prevention Device

By the late 1990s, it was common for "smart cards," laser cards, or other security cards or labels to be broken into, regardless of their technical sophistication. A report from the market analyst, Data Monitor, revealed that counterfeit card fraud rose by 121% from $95 million in 1999 to more than $211 million in 2003. An FBI Law Enforcement Bulletin in June 1997 said: "…counterfeiting a credit card has become a multi-step process, often using desktop computer systems and peripherals, including embossers, laminators, and

tipping foil, to produce a more realistic looking card, complete with a hologram and fully encoded magnetic strip." The New York Times reported on June 22, 1998 that a researcher had broken into electronic smart cards and had accessed secret data quite easily. Indeed, when smart cards were thus outsmarted, and other counterfeit prevention systems proved to be inadequate, manufacturers, consumers, and government agencies became very worried about transaction authenticity.

Every pair of blue jeans could have a tag that identified its manufacturer and brand.

If every product had an identifiable tag and every secure document had an authenticity tag, and neither tag could be counterfeited, prevention would be simple. For example, every pair of blue jeans could have a tag that identified its manufacturer and brand, and any fraudulent copies in the market could be rejected by the potential customer. Similarly, a credit card, identification card, or passport could have a secret code that could be authenticated. Such a solution to product counterfeiting and forgery was conceived by researchers at Physical Optics Corporation (POC) in the late 1990s. Their novel approach was based on a technology that POC called Optical Maximum Entropy Verification (OMEV). The technology incorporated concepts from statistical optics, pattern recognition, optoelectronic packaging, signal processing, manufacturing, and software development.

OMEV Is Smarter Than Smart Card

The OMEV concept used basic principles of optics and complex mathematics. When light falls on an object, patterns called optical fields are randomly scattered from the object because of the wave-like properties of light. This randomness in optical waves is called maximum entropy and can be analyzed by a mathematical formula called Fourier transform. Using the same principles, the optical patterns scattered from two objects can be quantified and compared in a process called cross-correlation. POC planned to use this concept for verification purposes. A laser-based system would randomly generate optical patterns on a polymer resin piece, called a mask, that acted as a master label. The authenticity of an unknown label could be verified by cross-correlating (comparing) its optical pattern with that of the master label in an OMEV optical correlator called a Joint Transform Correlator (JTC). Because the intricate patterns on the labels were randomly generated, POC claimed that the chances of these labels being forged were almost nil. Furthermore, the proposed OMEV labels would not contain redundant information that had exposed holograms to counterfeiting nor would they be reprogrammable, a characteristic that had increased smart cards' vulnerability to fraudulent usage.

POC Promises Huge Economic Pay-Off from OMEV

A cost/benefit analysis showed that OMEV technology could effectively reduce counterfeiting in the near term, thus saving the U.S. economy an estimated $24 billion annually. While the most immediate commercial applications for this system were in the area of product label verification, OMEV could benefit almost any part of the economy that was vulnerable to counterfeiting by protecting against fake products, fraudulent financial systems, and stolen identities. OMEV's capability to provide instant verification could dramatically enhance security in personal identification, banking, product label authentication, intellectual property protection, industrial and military security, document verification, and other applications. Additionally, the OMEV system would bring POC, a domestic company, into the U.S. market, which was dominated by foreign companies such as Siemens, Philips, and some Japanese firms.

OMEV Presents Significant Technical Challenges

POC planned to develop all critical components of the OMEV technology, including hardware and software; provide system integration; and develop a low-cost manufacturing technique for the labels and the reader. However, the complexity of OMEV masks and labels presented a variety of process and market-related challenges. There were significant technical hurdles in devising low- cost production processes for both the labels and the correlators. The proposed optical correlation technique had only been fabricated by the military in laboratory conditions. Commercialization had never been attempted, partly because of the prohibitive

costs involved. Researchers would also have to resolve any problems related to errors in correlation that could potentially cause authentic labels to be rejected as fake.

Because of the technical risks and the high level of innovation required, the OMEV project needed large financial resources that POC could not provide on its own. Therefore, they successfully applied for cost-shared funding from ATP, stating that ATP funding would expedite technical development by several years. The three-year research project was launched in October 1997, with the overall goal to develop anti-counterfeiting labeling technology based on optical pattern correlation.

Researchers Target Comparison and Authentication

The JTC would correlate (compare) a master label to an unknown mask or label to determine if they matched. If the JTC found them to be identical, the unknown label would be verified as authentic; otherwise the validating system would reject the unknown label. To use a simple analogy, the master label would function as a door lock and the authenticated label as a key. If the key opened the lock, the “door” would open and an authorized entry could take place. Specifically, the OMEV research project would develop two technologies:

- Non-replicable volume mask or label
- Novel optoelectronic verification system to verify the authenticity of the labels

Because the label was randomly generated, it could not be replicated easily. The verification system would only authenticate labels whose patterns matched pre-established, identical random patterns. Therefore, it would be almost impossible to produce fake labels.

ATP-Funded Project Achieves Early Successes

The POC team realized early in the research project that much of their work would be based on improving existing correlator technology. So, in the first quarter of the project, they developed the primary concept for a special correlator that would not only be able to compare labels quickly and reliably, but would be able to read the pattern on the unknown label and process the information even when the label was placed at an angle from the reader (was misaligned). The new correlator incorporated a laser light source, beam expander and splitter, Fourier transform lens, and a special camera. By passing a vertically polarized light beam from the laser through special lenses and a beam splitter, and then through clear resin plates, one beam of light illuminated the reference label and the other beam illuminated the unknown label being inspected. The beams were then transmitted through plates, which were mathematically analyzed by Fourier transform and recorded by the camera for correlation.

OMEV technology could effectively reduce counterfeiting in the near term, thus saving the U.S. economy an estimated $24 billion annually.

By October 1998, the POC team had built a computer simulation of a novel authentication technique for labels based on optical correlation. They also had developed various random sub-micron patterns for use on OMEV labels. In 1999, they designed a portable optical correlator and developed the software to run it. The portable correlator software charted the workflow for authentication; after one second of initializing, the software went through the steps to authenticate and accept or reject the label. Along with label verification, POC also built the capability for biometric signature authentication in these correlators. Biometric technology is used to measure and analyze human physical and behavioral characteristics such as fingerprints, facial patterns, voices, and signatures for authentication purposes.

POC Builds Prototype of JTC

Researchers built a JTC prototype that was ready at the end of the ATP-funded project. POC achieved its final project milestone with the design of optical hardware components, software components, and a testing system. They also evaluated the system for various market segments and explored several applications. The prototype correlator could compare the pattern of a master label with that of the unknown label to discern a match. The master phase masks were surface relief patterns etched in fused silica, as shown in Figure 1.

When a monochromatic beam of light was passed through a piece of resin, a volume phase mask was etched inside the resin, thus creating a label. Because it was etched inside the resin piece, rather than on its surface, only a JTC could read this phase mask pattern.

POC achieved its final project milestone with the design of optical hardware components, software components, and a testing system.

The phase mask could be attached to a product such as a computer chip, CD, or hard disk and could be read by the JTC to verify the product's authenticity. It looked like a piece of frosted glass with a two-dimensional array of values and information imaged inside the resin in a speckled pattern. The mask could not be removed without destroying the phase pattern, and thus the phase information could not be copied. If the optical pattern on a label was copied, the resulting mask would be of such poor quality that the correlator would reject it. Any attempt to tamper with the phase mask would also destroy it completely. This made the OMEV system tamper-proof and, hence, more effective than existing anti-counterfeiting systems.

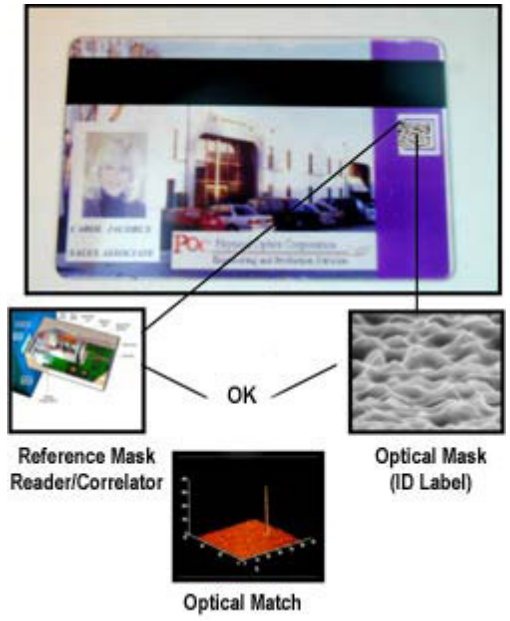

Figure 1. How the OMEV system worked

Two Key Components Make Up OMEV

Two key technologies emerged from this project: the novel correlator system and the phase mask technology. The OMEV-based system was promising because it resolved problems concerning cost, robustness, obsolescence, and unbreakability. POC received three U.S. patents and one patent from Taiwan[1] for its technology. After completing the ATP-funded research, the company identified the primary users of the OMEV system as shopping centers, hospitals, product manufacturers, credit card companies, and government agencies. In 2000, they initiated collaboration discussions with Raytheon, Motorola, Cryptek Secure Communication, and American Bank Note Company. They also continued to explore marketing opportunities for the OMEV technology, such as product manufacturers, credit card companies, and banks.

After the terrorist attacks on the World Trade Center in New York on September 11, 2001, it became apparent to both government and business that a more stable and unbreakable verification system was necessary in many fields. Whether it was used to enter into government buildings, protect personal data in identification cards, or safeguard important documents like a Social Security card, the verification system had to be quick, simple, trustworthy, and inexpensive, features that the OMEV system was promising.

Figure 2. Label Correlator

[1] "Authentication system and method," Taiwanese Patent No.154,372, granted April 21, 2002. The patent filed and granted in Taiwan was not included in the star rating calculation.

Therefore, in late 2001, POC saw an upsurge in interest for their product for the authentication of large volumes of data, encryption, and forgery prevention. But POC's existing correlator was too large for a portable device. Therefore, POC invested more research and development resources in building a new generation of readers and, in 2006, they created a correlator or label reader that was as small as 6x4x2 inches (shown in Figure 2). It could read a label on a piece of white plastic, similar to a credit card, rather than a clear resin card.

POC Receives Positive Response on Capitol Hill

POC developed the OMEV technology into a product for commercialization called the "Optikey system." The technology used to create the optical phase mask and its correlation for authentication was really like a unique optical signature recognition system: it was as if each product or document contained an optical signature that the correlator validated as authentic. Placed on labels, ID cards, or credit cards, the Optikey provided almost instantaneous verification, with or without linking to a central data bank or server. Furthermore, it could be enhanced by adding a biometric component to match signatures to users.

POC spun off a separate company, called Optikey, in 2005 to commercialize this product, and licensed the OMEV technology to them. As of 2006, the Optikey sales team had made two technical presentations to the U.S. House Appropriations Committee, several presentations to the U.S. Air Force, and another to a working group of the Motion Picture Association.

The commercialization of Optikey is focused in three areas: product verification in manufacturing industries, identity authentication in government agencies and controlled access areas, and legal replication in consumer electronics. Optikey can be used in a wide variety of applications, including military and civilian ID cards, passports, visas, Social Security cards, bank notes, credit and debit cards, card-entry door locks, electronic media like CDs and DVDs, airline baggage checking, and product protection. As of 2006, the company was actively soliciting business from leading credit card companies such as CitiBank and American Express to create an unbreakable authentication system for their credit cards. Considering that 30 percent of consumer fraud in 2005 was related to credit cards, and Visa International calculated as much as 5 percent fraud in a $1 trillion annual business in 2006, if Optikey could solve credit card fraud alone, it would offer a huge pay-back to the economy.

Placed on labels, ID cards, or credit cards, the Optikey provided almost instantaneous verification.

One of the biggest potential customers for Optikey is the Federal Government. Several agencies in the departments of Defense, State, and Homeland Security have expressed interest in this product, and the company has been pursuing these leads aggressively. The House of Representatives Appropriations Committee allocated $1 million for Optikey in the 2005 defense budget and an additional $1 million in the 2006 budget for integrating Optikey in controlled access cards issued by the U.S. Army and the Department of Homeland Security. The House has also shown interest in allocating additional resources in 2007 for use of Optikey by the Defense Information Systems Agency, the Defense Manpower Data Center, and the U.S. Air Force. In July 2006, the U.S. Government contracted with Lockheed Martin to provide an end-to-end solution for a fully secure, standard ID card for all Federal employees. As a subcontractor on this project, Optikey will deliver an enhanced security system based on the OMEV technology. Internationally, Optikey is involved in negotiations with a defense contractor to collaborate on an identification card for the European Union and other countries.

Optikey Projects Strong Business Outlook

Because product tags equipped with Optikey labels could be used to verify a wide variety of consumer items, this ATP-funded technology anticipates a strong potential market. Counterfeit products have been a serious problem for most manufacturers, as more companies lose revenue and market share to cheaper, illegal replicas of established brands. Optikey is collaborating with a security label manufacturing

company to produce as many as 50 million product tags in the form of 0.5 x 0.5 inch patches to be attached to products by 2007. These tags can authenticate products at different stages of the delivery process, including at the distributor level. The company is also working on design modifications for the label reader to make it smaller and more portable. The idea is to customize this system for each Optikey customer so that the patches can be attached easily during the assembly process, verified successfully during delivery, and remain virtually invisible to the end user.

The same kind of phase mask or label can be integrated into electronic media architecture for copy protection. To that end, Optikey is negotiating with Warner Bros. and Technicolor to apply this technology to DVDs and CDs. They are working with the Copy Protection Technology Working Group of the Motion Picture Association of America to formulate a methodology to prevent illegal copying of video and audio files.

Optikey registered total sales of $345,000 in 2005; only six months later, as of June 2006, sales had increased to $2.7 million. Demand for this technology is expected to grow substantially in the next few years, with projections reaching $11 million in 2007 and much higher in 2009.

Conclusion

Since the mid-1990s, counterfeit products, credit card fraud, and forged identity cards have taken a high toll on the U.S. economy and the country's security. Outdated authentication systems used by product manufacturers, financial companies, and government agencies have not solved these problems. Successive methods of verification and authentication have relied on either visual verification or digital encryption of information, which can be easily counterfeited. Physical Optics Corporation (POC) applied its experience in statistical optics, pattern recognition, and software development to develop a foolproof solution to forgery and product counterfeiting. Their novel approach is called the Optical Maximum Entropy Verification (OMEV) system. OMEV compared an optical pattern on a product label to a master phase mask or label and authenticated the product's legitimacy by matching the two. The matching was done by a correlator or reader using complex mathematical equations that made the label almost impossible to forge. POC received three patents for the OMEV technology in the United States and favorable reception from several companies and Federal agencies who have been interested in applying the technology to protect products, documents, and credit cards. Additional commercialization of the OMEV products by 2009 will have a huge impact on the ongoing fight to prevent product counterfeiting.

PROJECT HIGHLIGHTS
Physical Optics Corporation

Project Title: Optical Label and Reader to Prevent Counterfeiting (Optical Maximum Entropy Verification [OMEV])

Project: To develop an optical phase mask that can act as an identification label for products and documents and a correlator that can read the mask and compare it to a product label for verification.

Duration: 10/1/1997 - 9/1/2000
ATP Number: 97-01-0244

Funding (in thousands):

ATP Final Cost	$1,110	47.8%
Participant Final Cost	1,214	52.2%
Total	$2,324	

Accomplishments: Physical Optics Corporation (POC) accomplished all of its technical goals within the timeframe and plan set forth in their proposal to ATP:

- Developed the OMEV system
- Developed technology for a novel phase mask with a two-dimensional array of optical patterns etched in resin, which acted as a master label
- Developed a Joint Transform Correlator to read the optical pattern on a label and verify it with the pattern on the master label
- Improved the design of the correlator to make it usable at any point in the delivery process flow
- Developed an anti-counterfeiting prototype called Optikey for subsequent commercialization

POC received three patents from the United States and one from Taiwan for its ATP-funded technology. The U.S. patents are:

- "Method of making replicas while preserving master"
  No. 6,159,398: filed March 31, 1998, granted December 12, 2000
- "Composition for use in making optical components"
  No. 6,262,140: filed July 13, 1999, granted July 17, 2001
- "Authentication system and method"
  No. 6,744,909: filed August 19, 1999, granted June 1, 2004

POC received $2 million from the U.S. House Appropriations Committee for fiscal years 2005 and 2006 to integrate this technology into control access cards for the identification of defense personnel.

Commercialization Status: Based on the technology developed in the ATP-funded project, POC has developed the Optikey system, which is being actively commercialized by another company, called Optikey, to whom POC has licensed the OMEV technology. This company is actively negotiating the sale of Optikey products for product verification in manufacturing industries, identity authentication of government personnel and credit card users, and the legal replication of consumer media by consumer electronics companies.

Outlook: The Optikey system had sales of $345,000 in 2005 and $2.7 million by June 2006. Demand is expected to grow substantially in the next few years, with projected sales reaching $11 million in 2007 and $88 million in 2009. The outlook for this technology is very strong.

Composite Performance Score: * * *

Number of Employees: 90 employees at project start, 135 as of June 2006.

Company:

Physical Optics Corporation
20600 Gramercy Place
Torrance, CA 90501

Contact: Rick Shie
Phone: (310) 320-3088

Presentations:

- Schroer, W &Jon Paul Javellana. Optikey and Copyright Protection in DVDs. *Motion Pictures Association of America*, Los Angeles, CA. 2005
- Schroer, W. Optikey Applications. *U.S. Congress*, Washington, D.C. 2006.
- Schroer, W. Optikey Application in Restricted Entry Identification Cards. *U.S. Air Force*, Washington, D.C. 2006
- Schroer, W. Optikey Applications . Department of Culture, Government of UK, London, England 2006.