

# A Survey of Current Optical Security Techniques

Ari Y. Benbasat  
MIT Media Lab

Prepared for Prof. Cardinal Warde  
6.637 Spring 1999 Research Project

April 15, 1999

## **Abstract**

In this paper, we describe two types of optical security devices: diffractive anti-counterfeiting devices such as holograms and microgratings, and encryption techniques such as double-phase encoding and optoelectronic implementation of conventional algorithms.

It is shown that holograms are more easily copied than is widely believed, though advanced techniques may soon make duplication far more difficult. Zero-order microgratings, which produce a distinctive red to green colour shift upon rotation about their own axis, are offered as a more secure alternative that could gain ascendancy.

Double-phase encryption allows for simple encoding using a two-lens processor, as well as the possibility of denser holographic storage. Its security, however, is poor because of its linearity. Optoelectronic implementations of operations such as exclusive-or and bit-permutation, which are central to current cryptography, will allow faster parallel instantiations of algorithms for which the security is already well tested.

# Contents

<b>Abstract</b>	<b>ii</b>
<b>List of Figures</b>	<b>iv</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Topics Covered . . . . .	1
1.2 Topics Not Covered . . . . .	1
<b>2 Diffractive Optical Security Techniques</b>	<b>3</b>
2.1 Holography . . . . .	3
2.1.1 Basic Technique . . . . .	3
2.1.2 Ease of Counterfeiting and other Drawbacks . . . . .	4
2.1.3 Copy Resistance Techniques . . . . .	5
2.2 Zero Order Diffraction Microgratings . . . . .	6
2.2.1 Theory and Implementation . . . . .	6
2.2.2 Copy Resistance and other Features . . . . .	8
<b>3 Optical Cryptographic Techniques</b>	<b>9</b>
3.1 Double-phase Encoding . . . . .	9
3.1.1 Implementations and Uses . . . . .	9
3.1.2 Analysis of Security . . . . .	11
3.2 Optoelectronic Methods . . . . .	12
3.2.1 Implementations and Uses . . . . .	12
3.2.2 Analysis of Security . . . . .	14
<b>4 Discussion of Impact/Applications of Techniques</b>	<b>15</b>
4.1 Diffractive Techniques . . . . .	15
4.2 Cryptographic Techniques . . . . .	16
<b>5 Summary</b>	<b>18</b>
<b>References</b>	<b>20</b>

## List of Figures

1	The recording (a) and playback (b) of a rainbow hologram . . .	4
2	Single step of two-step hologram copying procedure . . . . .	5
3	Dielectric structure of a simple zero order micrograting . . . .	7
4	Reflectance for parallel ( $E_p$ ) and perpendicularly ( $E_s$ ) polar- ized light . . . . .	7
5	Encryption using a two-lens processor . . . . .	10
6	Decryption using a two-lens processor . . . . .	11
7	Two-input optical XOR gate with possible states. . . . .	13

## 1 Introduction

The subject of optical security techniques is a very broad one, and one that is enjoying increasing prominence. Conventional reproduction techniques (*eg.* photocopiers) have been increasing in quality steadily for the last thirty years, and therefore necessitate innovative countermeasures to counterfeiting. Also, in the last decade, the importance of cryptography has risen greatly with the expansion of public communication systems. The coincident rise of optical (usually holographic) memories has created a burgeoning field of optical only and optoelectronic encryption.

The sheer number of these techniques, however, is daunting. Therefore, a small subset has been chosen for inclusion in this paper. While the author makes no claim as to the overweening importance of the topics chosen, it is hoped that they represent some of the more interesting and useful techniques available.

### 1.1 Topics Covered

The techniques covered in this document are divided into two major categories. The first are anti-counterfeiting techniques. In this area, we have chosen to examine both a first order structure, holograms, which are fairly well known, and a zero order structure, diffractive microgratings, that are not yet in common usage. These are discussed in Section 2.

The second category of techniques covered are optical cryptographic techniques. In this case, we examine both purely optical (Fourier plane) methods, as well as optoelectronic implementations of conventional algorithms. These are covered in Section 3.

Furthermore, a discussion of the future impact of these techniques can be found in Section 4, and a summary is presented in Section 5.

### 1.2 Topics Not Covered

There are a number of topics in this field that, while interesting, are not covered for a variety of reasons. Intaglio printing, while ubiquitous, is a technique whose security rests solely in the difficulty of production, rather

than in any interesting optical effect that it may produce. Techniques such as watermarking and microprinting also fall into this category. The reader is directed to [1] if they are interested in these fields.

Kinegrams and pixelgrams[2] (both first order structures), while showing great promise and increasing use, are omitted because they enjoy nowhere near the market penetration of holography.

Several encoding topics should be mentioned here but are not covered in the main document. Stenography[3] is considered a superset of cryptography (since the message hidden is usually encrypted) while keystream generation[4] is a (admittedly important) subset of cryptography. Both were excluded in favour of greater coverage of the core topic.

## 2 Diffractive Optical Security Techniques

Diffractive structures are the core of modern optics, the basis of everything from holograms to spatial light modulators. These structures have a wealth of useful features, not the least of which is their ability to produce images which cannot be reproduced through photographic means. While this is often due to their three dimensional appearance, it can also result from various other chromatic effects.

In this section, two major topics are covered. The first is the well known field of holography, the second is the much lesser known field of diffractive microgratings.

### 2.1 Holography

The technique of wavefront reconstruction, first proposed by Gabor in 1948 and now known as holography, is well-known for its ability to produce beautiful three dimensional images unobtainable through conventional photography. For almost this reason alone, they have been a cornerstone of the anti-counterfeiting industry for 20 years. The formation of holograms is detailed below. A number of techniques for duplicating holograms will be explored, and a few methods of making copy resistant holograms will be discussed.

#### 2.1.1 Basic Technique

While the basic techniques of holography are well known, they bear review here. Those interested in a more in depth review of the field and its various techniques are directed to [5].

The technique most often used to create anti-forgery holograms is that of rainbow holography. A key benefit of this process is that they can be reconstructed under white light. The recording process is shown below in Figure 1 (from [6]). A conventional transmission hologram  $H_1$  of the desired object is first created. This hologram is then played back through a thin horizontal slit, and the real image is written onto a second holographic plate  $H_2$ . If this hologram is then played back with white light, both a real image of the slit and a virtual image of the original object will be reconstructed. A monochromatic image of the object will be visible “through” the slit. Moving the field

of view vertically will alter the playback colour (hence the name rainbow hologram), while moving the field of view horizontally will result in the usual parallax that is a key characteristic of holograms. The three dimensionality that is courtesy of this parallax and the colour change upon vertical shift are the key security features of this device.

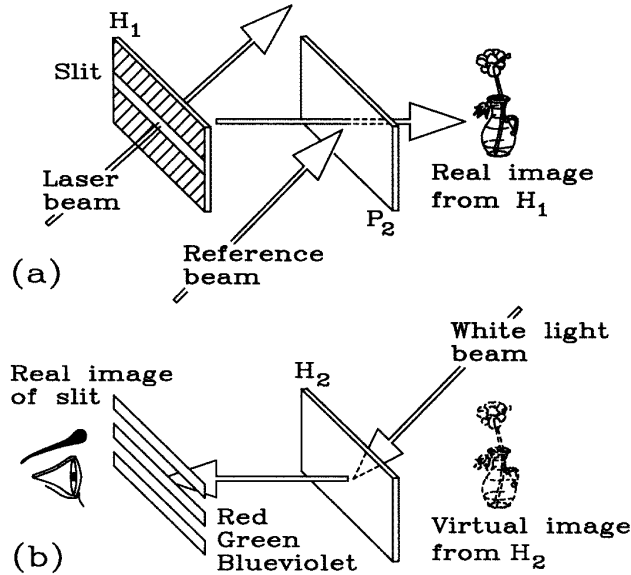


Figure 1: The recording (a) and playback (b) of a rainbow hologram

### 2.1.2 Ease of Counterfeiting and other Drawbacks

Despite their famed resistance to photographic reproduction, holograms can be easily duplicated in a number of different fashions. The simplest technique is the use to hologram itself to make a negative mold, which can then be used to press an unlimited number of virtually perfect duplicates (positives). If access to the substrate is not available (as is the case with credit card mounted holograms) a new hologram can be recorded from the output of the first (Figure 2) [7]. This is done by simply illuminating the first hologram with the reference beam (which is almost certainly one of a small number of wavelengths in which production lasers are available) and then recording an intermediate hologram with the output. The final duplicate hologram is then

made from the intermediate in the same fashion (the two-step process is necessitated by the mirroring of the output in holography). While the results of the process will not be perfect, it will be accurate enough to fool the end-user.

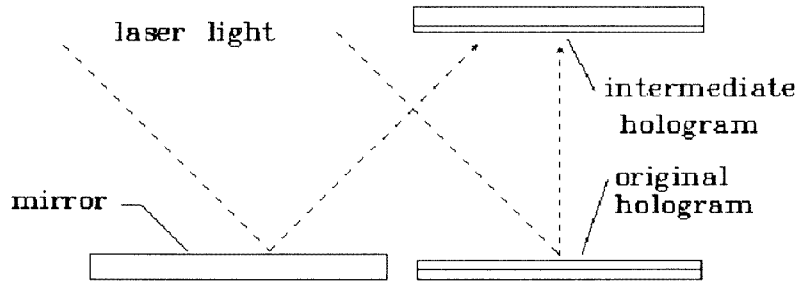


Figure 2: Single step of two-step hologram copying procedure

Other methods are also tenable, though there is a reluctance in the field to publish them in the open literature. However, it is the view of the author that the lack of easily available references will not deter a smart counterfeiter very long, and will leave legitimate users unable to accurately gauge the risks involved in trusting holograms as security devices. That being said, [7] and [8] are given as good sources of other techniques.

A second drawback of holograms is that since they are first order diffractive objects, the quality of the output will be a function of the directionality of lighting in the vicinity. Therefore, their output will range from clear and sharp under collimated light (such as a reading lamp) to very blurry under diffuse light (such as fluorescent bulbs and an overcast sky).

### 2.1.3 Copy Resistance Techniques

A number of techniques exist to make holograms harder to copy. The most obvious method is to make it impossible to separate the hologram from its substrate, the necessary first step to mechanical reproduction. The use of complicated images can make it more difficult for a forgers to reconstruct the hologram from scratch (see also note below). Both of these techniques are in common use.

However, the strongest copy prevention technique is the use of so-called see-through holograms, which are made as follows[8]. A conventional hologram is created and then coated with a reflective backing. This backing is selectively varnished and then bathed in an acid bath, which removes the unvarnished backing resulting in a hologram with somewhat reduced reflectivity. The key to the process is that this hologram is then laid on top of a second (conventional) image. A viewer will either be able to see the substrate image or the hologram (depending on the angle of incidence), but not both. Attempts to copy a see-through hologram as described above will come away with only the image of the still reflective portion. This image would then have to be re-metallized only at the exact same points as before, a process which requires a heroic level of accuracy which is currently unobtainable.

It is also worth noting that the ability of a hologram to produce a fairly high quality image of the human face is considered by a large percentage of the community to be a security feature. This is based on the anecdotal ability of human beings to detect minute differences in facial structure[8], which would therefore require duplicates to be of much higher quality. Others[2] have pointed out that there is no formal literature on the topic, and, moreover, that humans have the ability to recognize even greatly distorted faces, which would tend to counter any possible benefit of their use.

## **2.2 Zero Order Diffraction Microgratings**

The second diffractive technique that will be discussed are zero order diffractive microgratings. These are structures with a characteristic length less than that of visible light, so only specular reflection (as modified by the structure) will be present. It will be shown that these microgratings have certain optical properties that are not seen in other devices.

### **2.2.1 Theory and Implementation**

A zero order micrograting is simply a regular diffractive structure with a characteristic length in the hundreds of nanometers. An example of such a structure is shown in Figure 3 (from [9]). A rigorous solution of Maxwell's equations for this layout will render a number of surprising properties. The first is that the structure has a very pronounced reflectance peak in the red

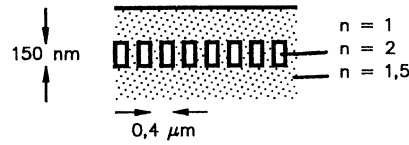
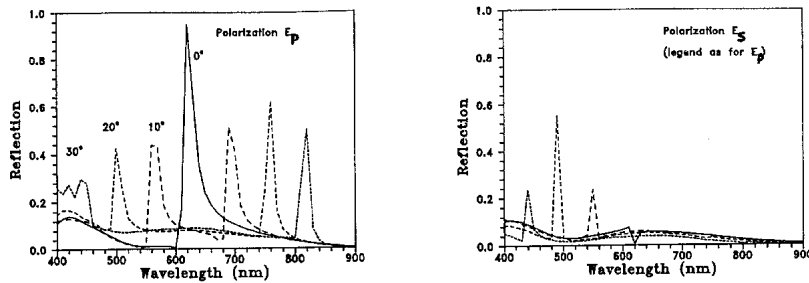


Figure 3: Dielectric structure of a simple zero order micrograting

portion of the spectrum at normal incidence. This peak will split and shift linearly with angle of incidence, leaving the visible range at  $\sim 30^\circ$ . The second, and more important, property is that light polarized parallel to the grating lines will have a different reflectance than light polarized perpendicular to the grating lines, this time peaking in the green portion of the spectrum. These peaks are shown in Figure 4 (again from [9]). Therefore, rotating this structure about its own axis will result in a colour change from red to green, a unique property that is its key security feature.

Figure 4: Reflectance for parallel ( $E_p$ ) and perpendicularly ( $E_s$ ) polarized light

It turns out that these structures can be fairly easily manufactured in large quantities[10]. Furthermore, since they can be made solely out of plastics, these micrograting can be embedded within a security device during the manufacturing process, rather than affixed on top afterwards as with holograms.

### **2.2.2 Copy Resistance and other Features**

Zero order microgratings offer great resistance to duplication. Obviously, they cannot be copied photographically since they are non-static, and holographic copying techniques are inapplicable. In contrast to holograms, however, the structure of the grating is fairly simple and will likely be widely known. Forgery is still assumed to be unlikely for a number reasons. The first is that the manufacturing capability necessary to make the structure is very expensive[10], far more than that required to duplicate holograms. The second is that since the grating can be embedded within the security device, a forger would have to duplicate that as well. Finally, since this structure is very well suited to machine-verification[11] (usually of the reflectance), the duplicate would have to be of very high quality. This combination of factors should render counterfeiting less than cost-effective.

Also, note that since this is a zero order device, it will, by definition, not suffer from the overlapping first orders that tend to blur hologram images. Therefore, it should be clearly viewable under all lighting conditions[2].

## 3 Optical Cryptographic Techniques

Cryptography, once a fairly obscure field, has risen greatly in importance with the recent increase in public communication systems and a newfound interest in personal privacy. Recent work in the field has investigated the possibility of optical only and optoelectronic encryption, and some very interesting results are described below.

### 3.1 Double-phase Encoding

Two-lens classical processors and VanderLugt correlators[5] have been staples of optical information processing for the last 30 years. Recently, a number of novel cryptographic algorithms incorporating these devices have been proposed. The most mature technique, double-phase encoding, will be explained, and its security will be commented upon.

#### 3.1.1 Implementations and Uses

The simplest, and most useful, classical processor based encryption scheme is due to Refregier and Javidi[12] and is shown in Figure 5 (from [13]). The theory is fairly straight-forward. The original image  $f(x, y)$  is multiplied by a random (known) phase mask  $\exp\{i2\pi p(x, y)\}$ . A second random phase mask,  $\exp\{i2\pi b(\alpha, \beta)\}$ , is placed in the Fourier plane (where  $\alpha, \beta$  are conjugate variable to  $x, y$ ) and is the key. The output is then:

$$\Psi(x, y) = [f(x, y) \exp\{i2\pi p(x, y)\}] * \mathcal{F}^{-1}[\exp\{i2\pi b(\alpha, \beta)\}] \quad (1)$$

where  $*$  denotes the convolution operator and  $\mathcal{F}^{-1}$  is the inverse Fourier transform. It can be shown[12] that the output will have the properties of stationary white noise.

Decryption is simply the inverse operation (Figure 6 [13]).  $\Psi(x, y)$  is the processor input, and the conjugate of the key ( $\exp\{-i2\pi b(\alpha, \beta)\}$ ) is placed in the Fourier plane. We see that the output is:

$$\begin{aligned} g(x, y) &= \Psi(x, y) * \mathcal{F}^{-1}[\exp\{-i2\pi b(\alpha, \beta)\}] \\ &= [f(x, y) \exp\{i2\pi p(x, y)\}] * \mathcal{F}^{-1}[\exp\{i2\pi b(\alpha, \beta)\}] \\ &\quad * \mathcal{F}^{-1}[\exp\{-i2\pi b(\alpha, \beta)\}] \\ &= [f(x, y) \exp\{i2\pi p(x, y)\}] * \delta(x, y) \end{aligned}$$

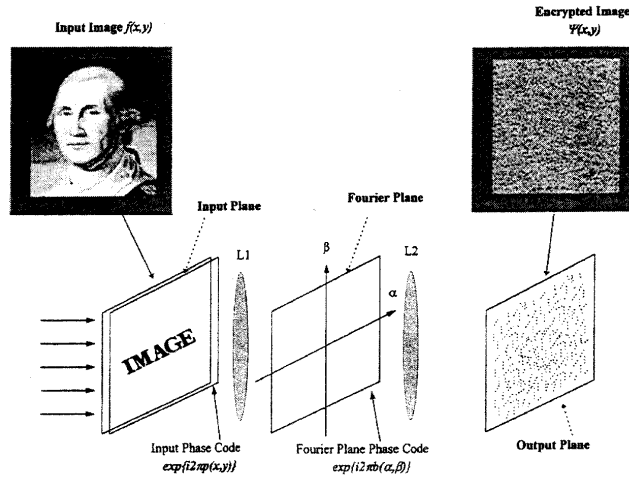


Figure 5: Encryption using a two-lens processor

$$= f(x, y) \exp\{i2\pi p(x, y)\} \quad (2)$$

The random phase will disappear when the image is recorded with an intensity sensitive device. Alternatively, the input phase can be removed by placing its conjugate in the output plane and the decrypted image can then be compared to expected image using a VanderLugt correlator. Note that the recovered image is nearly perfect and the output is still fairly sharp in the presence of white noise[12].

Note that the phase masks can be implemented in several ways. If only a static (single key) version of the system is desired, appropriate transparencies would be adequate. For an adjustable system, spatial light modulators can be used to create variable phase masks.

A useful feature of this setup is that the encrypted image can be written directly into a holographic memory. Since the system is resistant to noise, it is possible to store multiple overlapping images (with the same reference beam) on a single film, with a different key used for each. The individual images can then be recovered, with the unwanted images entering the analysis as white noise[14] (calculations of the signal to noise ratio can also be found in this reference).

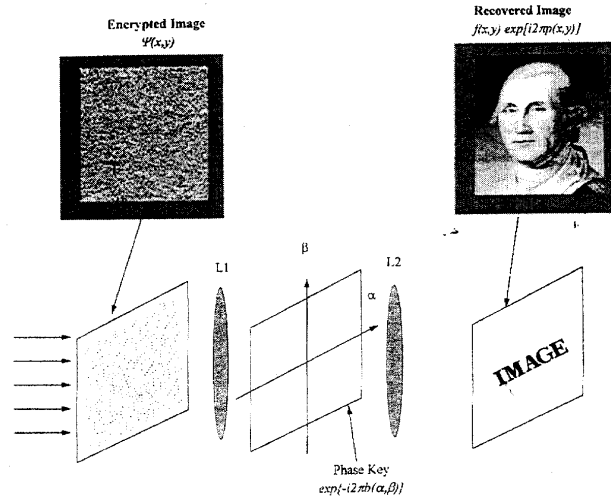


Figure 6: Decryption using a two-lens processor

### 3.1.2 Analysis of Security

The security of this method, sadly poor. While there are some statements as to its apparent security, there is nothing in the literature that approaches a formal proof. Furthermore, its linearity opens several avenues of attack.

The few statements of security of this algorithm centre on the fact that the encrypted data has the form of stationary white noise (the random input phase is required for this property). While this may be true, it is no guarantee of security. Almost every major cypher has this property[15], and some of them are quite insecure. Also, tests showing that a very small number of keys chosen from the keyspace fail to properly decrypt an encrypted image (such as in [14]) are of little value, since this offers no assurances that other randomly chosen keys will similarly fail.

The key flaw in this algorithm is that it is a linear system, which allows a number of attacks that would not be possible in non-linear algorithms. For example, if the same key is used to encode multiple image (as suggested in [12]), attackers can take advantage of the correlation between two (or more) encrypted images to find the key (this assumes only a modicum of struc-

ture in the original images). Worse yet, if one of the unencrypted images is somehow disclosed, the key can be found as follows. First, take the Fourier transform of the encrypted image and conjugate it. Place this in the Fourier plane of a two-lens processor and place the unencrypted image in the input plane. The Fourier transform of the output will then be:

$$\begin{aligned}
 g(\alpha, \beta) &= \mathcal{F}[f(x, y) \exp\{i2\pi p(x, y)\}] \mathcal{F}^*[\Psi(x, y)] \\
 &= \mathcal{F}[f(x, y) \exp\{i2\pi p(x, y)\}] \mathcal{F}^*[f(x, y) \exp\{i2\pi p(x, y)\}] \\
 &\quad \times \exp\{-i2\pi b(\alpha, \beta)\} \\
 &= \exp\{-i2\pi b(\alpha, \beta)\}
 \end{aligned} \tag{3}$$

where we have assumed that  $f(x, y)$  is normalized (or have done so). Note that we now have the key and can decrypt any other message that was encoded with it. Therefore, this algorithm is only secure if key material is never reused, which is a fairly stringent requirement. Also, note that this technique is to some extent immune to multiplicative and additive white noise[16]. This implies that each output pixel is not a function of every input pixel, which would tend to make iterative key guessing attacks much less complex.

## 3.2 Optoelectronic Methods

There is, of course, already a rather large body of cryptographic algorithms. If their core operations can be implemented optoelectronically, it would then be possible to exploit cyphers which are already known to be well resistant to attack.

### 3.2.1 Implementations and Uses

A quick survey of major symmetric encryption algorithms will show that they tend to be composed of a bit-wise logical operators (mostly exclusive-or), bit-permutations and lookup tables. Each of these can be implemented with varying degrees of ease.

A two-input exclusive-or (XOR) gate can be implemented very simply using two polarizers and two liquid crystal displays (Figure 7)[17] as follows. Note first that an LCD that is switched on will rotate light by  $90^\circ$ , while one that is switched off will simply pass the light. One arbitrary polarization

(in this case, horizontal) is designated to be 1, while the other (vertical) is zero. Unpolarized light is then passed through a “0” polarizer, then through two LCDs which are either on or off depending on their input value, and then outputted through a “1” polarizer. If the light passes through exactly one LCD which is switched on, it will be able to pass through the output polarizer and is considered a 1 output. If it passes through either zero or two polarizers which are switched on, it will not be able to pass through the output polarizer and will be considered a 0. It is evident that this scheme can be trivially extended to an arbitrary number of inputs. All other logic gates can also be implemented optically. The reader is directed to [18] for more details.

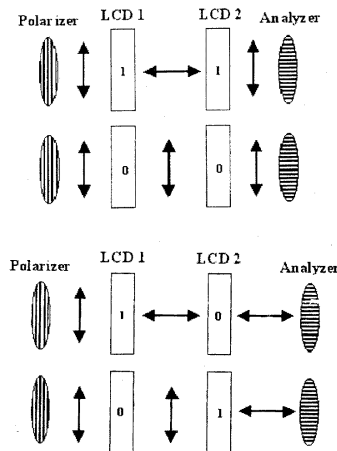


Figure 7: Two-input optical XOR gate with possible states.

The optical structures to produce look-up tables are fairly involved, and are described in [19]. This paper also describes how to create bit-permutations, which are simply appropriate lens structures, and details an optical implementation of the U.S. Data Encryption Standard (DES)[15].

Note that a number of implementations (such as [17]) in the literature simply XOR the data with the key as a method of encryption. While far simpler to implement than DES, it is insecure for reason discussed below.

The majority of asymmetric (public key) encryption algorithms are based around modular exponentiation. While this operation can be decomposed into a sequence of logical operators (in fact, any computer operation can), it is likely that the algorithm will become very cumbersome to implement in optoelectronic hardware at this point.

The major benefits of optoelectronically implemented cryptography is that a vast number of operations can be run in parallel very quickly in a relatively straight-forward and cost-effective manner compared to similar operations in electronics.

### 3.2.2 Analysis of Security

Since these algorithms are identical to those already in use, and there is no obvious change in security attributable to optical implementation, they will have the same security. Specifically, XOR-only encryption schemes (as with double-phase encoding) will be perfectly secure if and only if the key data is perfectly random and never reused (*ie.* a one-time pad); otherwise, correlations between blocks encoded with the same key can be exploited to easily break the encryption[15]. DES itself is reasonably secure against most attackers, however, those with medium resources ( $\sim$  \$250,000) can decrypt a message through brute force in an average of 2 days[20]. Chaining three DES operations together produces a cypher known as 3DES with a 168 bit key which is unlikely to be guessed in the lifespan of the universe[15].

## 4 Discussion of Impact/Applications of Techniques

The techniques detailed above range greatly in terms of current and future impact and utility, and these topics bare discussion. The impact of these technologies will be discussed in the case of the diffractive techniques, while the possible applications and utility will be discussed for the cryptographic techniques.

### 4.1 Diffractive Techniques

Both holograms (first order) and diffractive microgratings (zero order) are described above. Broadly stated, holograms are very much the security technology of today, while microgratings are very likely the technology of the future.

Holograms currently enjoy great penetration in the marketplace. They are used as an anti-forgery device on everything from high value items such as credit cards to mass merchandise items such as sport memorabilia. People understand (to some extent) what a hologram is and what properties it has compared standard (two-dimensional) images. This popular knowledge is a key part of what makes them an effective device. However, holograms are fairly easy to counterfeit. The lack of popular knowledge of these duplication techniques helps maintain their trust level. It is only a matter of time before a motivated party is able to perpetrate wholesale fraud with duplicated holograms, and possibly shake consumer confidence.

If, at the time that holographic security is called into question, zero order micrograting have achieved some (even relatively minor) level of general use, they should be able to vault to a position of dominance. These structures have properties that are as distinctive as those of holograms, and the fact that they are somewhat simpler to describe may be of aid to the (fairly uneducated) end-user who has to decide of an object is authentic.

Of course, there are open questions that were not addressed in the vision above. If see-through holograms gain widespread use, it is unlikely that anyone will be able to effectively duplicate them and thus spur their decline.

Also, the security of microgratings is reasonably untested. It may be possible that advances in production techniques will render their duplication very cost effective. It is also possible (though unlikely) that other structures that produce a similar colour change on rotation may be found. Any of the above would help holograms maintain their current entrenchment, at least until another clever technology came along.

## 4.2 Cryptographic Techniques

Most of the possible applications of optoelectronic cryptography stem from its ability to deal with light and images in their natural environment. As a simple concrete example, consider an identification card that not only contained the owner's name, but also an encrypted version of their fingerprint. The card is validated by decrypting the image of the fingerprint and using it as one input to a joint transform correlator[21] whose second input is a live image of the print. All of the processing in this system is done through simple optical constructs, with the output being a very easily detected correlation peak. No CCD or other complicated hardware, no pattern recognition or other complicated software required.

If holographic memories fulfil their current promise and succeed in providing ultra-dense storage, a scheme such as double-phase encryption will prove enormously valuable since it would allow everything to be encrypted just prior to storage and decrypted upon retrieval. The key itself would be stored in a small amount of static RAM which could travel with the user, thereby providing greater security. Note that this scheme also avoids one of the greatest problems of current cryptographic implementations, which is that since encryption requires a specific effort on the part of the user, only important files are encrypted. These files are then easily distinguished from unencrypted (and therefore unimportant) files, making an attacker's work easier.

The value of transparent, low-level encryption cannot be underestimated. Such implementations provide a fairly high level of security at the cost of little design effort and no with thought on the users part. Currently, packet-level encryption is available on internet routers. Considering that both internet data and voice (phone) signals are carried on the same physical infrastructure, fiber optics, it is not inconceivable that some optical processing scheme

could secure both with an even greater level of transparency.

However, these visions of the future all rely on encryption schemes that are more secure than the ones presented in this paper. For example, double-phase encryption of optical memory using only a single key could be broken as described above through the use of known data blocks (such as required operating systems files, etc.). The creation of stronger algorithms would require a fairly large paradigm shift in the way research in optically-based encryption is done, bringing it more in line with the rigorous mathematics of conventional cryptography. The first step would be the cryptanalysis of the current methods and a formal calculation of their strength based on key size. Also, it should be noted that all of the current algorithms apply solely to fields of static data, and are therefore inapplicable to the time-varying pulses of fiber optic communication. Nonetheless, the potential in these techniques is great enough to make this an enormously valuable field of inquiry.

## 5 Summary

In this paper, two different types of optical security devices were considered. The first was diffractive optical devices, in which holograms (a first order structure) and diffractive microgratings (a zero order structure) were considered. The second was optical cryptographic techniques, where both double-phase encoding encryption and optoelectronic cryptographic implementations were examined.

The creation of rainbow holograms, the anti-counterfeiting device most widely used today, was detailed. It was shown that these devices produce very distinct images, which show both parallax (leading the three-dimensionality) when moved horizontally and colour shift when moved vertically. Unfortunately, these objects are fairly easy to duplicate, and several methods to do so were detailed. See-through holograms, in which part of the reflective coating is etched away to allow viewing of an image underneath from certain angles, promises to make forgery far more difficult.

Diffractive microgratings have a characteristic length of less than the wavelength of visible light, and therefore produce only zero-order (specular) light. Certain well chosen grating patterns will result in very distinct properties, which stem from different reflectances for light polarized parallel and perpendicular to the grating. These properties include a bright peak centered on the red part of the spectrum at normal incidence and shifting to green at about  $30^\circ$  incidence and a colour change from red to green upon rotation about its own axis. These objects were deemed superior to holograms because of their resistance to counterfeiting and their simple yet distinct properties.

Double-phase encoding encryption is a simple, optical only method of image encoding using a two-lens classical processor. Random phase masks are placed over both an input image and in the Fourier plane. The first mask is disclosed, the second can be thought of as the secret key. The encrypted output has the characteristics of stationary white noise. Decryption is achieved by simply placing the encrypted image in the input plane and the conjugate of the key mask in the Fourier plane. Because this technique is robust under white noise, multiple images encoded with different keys can be stored in a single hologram. However, the overall security of this method is poor due to attacks based on its linearity.

Conventional encryption algorithms can be implemented optoelectronically. It is shown how an exclusive-or gate can be built by exploiting the polarizing properties of liquid crystal displays. Look up tables and bit-permutations can also be implemented, though only through more complicated techniques. The value of implementing conventional algorithms in this fashion is that they now can be run very quickly and easily in parallel and that their well-documented security can be exploited.

The future impact and applications of these devices was discussed. Given the ease of counterfeiting of holograms, it seems likely that they will eventually (likely following a very news-worthy forgery) be superseded by zero order gratings, unless the more secure see-through hologram comes into wider use. Optical encryption techniques could be coupled with holographic memories, thereby producing dense storage in which all data is trivially and efficiently encrypted just prior to storage and decrypted upon retrieval. Encryption of all data transmitted on fiber optic networks at the transmission stage is also a possibility. However, a paradigm shift, both in the way these encryptions are done and in the quality of the proofs of their security would first be required.

## References

- [1] J. Haslop, "Security Printing Techniques," in *Optical Document Security*, R. van Renesse, Ed., Artech House, Norwood, MA (1993).
- [2] R. van Renesse, "Iridescent Optically Variable Devices: A Survey," in *Optical Document Security*, R. van Renesse, Ed., Artech House, Norwood, MA (1993).
- [3] Y. Desmedt, S. Hou and J-J. Quisquater, "Audio and Optical Cryptography," *Proc. ASIACRYPT '98 (LNCS 1514)*, 392-404 (1998).
- [4] J-W. Han, S-H. Lee, and E-S. Kim, "Optical key bit stream generator," *Opt. Eng.* **38**(1), 33-38 (1999).
- [5] J. Goodman, *Introduction to Fourier Optics*, 2nd ed., McGraw Hill, New York (1996).
- [6] R. van Renesse, "Introduction to Optical Document Security," in *Optical Document Security*, R. van Renesse, Ed., Artech House, Norwood, MA (1993).
- [7] S. McGrew, "Hologram Counterfeiting: Problems and Solutions," *Proc. SPIE* **1210**, 66-76 (1990).
- [8] G. Colgate, "Document Protection by Holograms," in *Optical Document Security*, R. van Renesse, Ed., Artech House, Norwood, MA (1993).
- [9] M. Gale, K. Knop and R. Morf, "Zero-order diffraction microstructures for security applications," *Proc. SPIE* **1210**, 83-89 (1990).
- [10] M. Gale, "Replication Tehcnology for Holograms and Diffractive Optical Elements," *J. Imag. Sci. and Tech.* **41**(3), 211-220 (1997).
- [11] M. Gale, "Zero-Order Grating Microstructures," in *Optical Document Security*, R. van Renesse, Ed., Artech House, Norwood, MA (1993).
- [12] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**(7), 767-769 (1995).

- [13] B. Javidi, "Optical Information Processing For Encryption and Security Systems," *Proc. SPIE* **3075**, 122-127 (1997).
- [14] B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double-random phase encoding," *Proc. SPIE* **3384**, 130-136 (1998).
- [15] B. Schneier, *Applied Cryptography*, 2nd ed., John Wiley, New York (1994).
- [16] B. Javidi, "Noise performance of double-phase encryption compared to XOR encryption," *Opt. Eng.* **38**(1), 9-19 (1999).
- [17] J-W. Han, C-S. Park, D-H. Ryu, and E-S. Kim, "Optical image encryption based on XOR operations," *Opt. Eng.* **38**(1), 47-54 (1999).
- [18] A. Khan and U. Nejib, "Optical logic gates employing liquid crystal optical swithces," *Opt. Eng.* **26**(2), 270-273 (1987).
- [19] M. Schmalz, "Optical and electro-optical architectures for the compression and encryption of discrete signals and imagery," *Proc. SPIE* **2238**, 121-130 (1994).
- [20] J. Gilmore, ed., *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*, O'Reilly, New York (1998).
- [21] B. Javidi and J. Horner, Eds., *Real-time Optical Information Processing*, Academic Press, San Diego (1989).