Technological University Dublin
ARROW@TU Dublin

Books/Book Chapters

Centre for Industrial and Engineering Optics

2020

Holographic security

Vincent Toal
Technological University Dublin, vincent.toal@tudublin.ie

Follow this and additional works at: https://arrow.tudublin.ie/cieobk

 Part of the Optics Commons

Recommended Citation

Vincent Toal, Chapter 8 - Holographic Security, Editor(s): Pierre-Alexandre Blanche, Optical Holography, Elsevier, 2020, Pages 191-206, ISBN 9780128154670, DOI: 10.1016/B978-0-12-815467-0.00008-6.

This Book Chapter is brought to you for free and open access by the Centre for Industrial and Engineering Optics at ARROW@TU Dublin. It has been accepted for inclusion in Books/Book Chapters by an authorized administrator of ARROW@TU Dublin. For more information, please contact arrow.admin@tudublin.ie, aisling.coyne@tudublin.ie, gerard.connolly@tudublin.ie.

This work is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 4.0 License

TABLE OF CONTENTS

8 HOLOGRAPHIC SECURITY 2

8.1 Introduction 2

8.2 The counterfeit problem 2

8.3 Holographic security and authentication 3

8.4 Mass produced holograms 3
8.4.1 Rainbow holograms 3
8.4.2 Volume reflection holograms 4

8.5 Serialised holography 5

8.6 Fourier methods for image comparison 5
8.6.1 Optical matched filtering 5
8.6.2 Joint transform correlation 7

8.7 Encryption methods in holography 8
8.7.1 Phase coded reference beam encryption 8
8.7.1.1 Random phase encoding 8
8.7.1.2 Deterministic orthogonal phase coding 9
8.7.2 Double random encryption 10
8.7.3 Polarization encryption 11
8.7.4 Fractional Fourier encryption 11
8.7.5 Fresnel domain double random phase encryption 12

8.8 Digital holographic security 12
8.8.1 Phase shift digital holography 13
8.8.1.1 Two phase shifts 13
8.8.1.2 Partitioned SLM 14
8.8.1.3 Quadrature phase shift modulation 14

8.9 Holography for imaging of concealed objects 15

8 Holographic security

Abstract

This chapter is concerned with the security applications of holographic techniques. Holograms are used in product authentication, product branding and brand protection and personal and other documents. Serialisation to ensure the uniqueness of each hologram for added security, is briefly discussed.

The theory of optical character recognition and joint transform correlation methods is outlined.

Holographic recording using encrypted reference waves enables secure storage of information. Several methods are considered for encrypting optical data well as holographic recording of encrypted images and their reconstruction and decryption.

Millimetre and microwave holographic imaging techniques for the detection of hidden contraband, narcotics, firearms and explosives are also discussed.

Keywords: authentication, holography, white light holography, serialisation, optical matched filters, reference beam coding, spatial encryption, phase shift digital holography, microwave holography

8.1 Introduction

The wavelength and spatial distribution of amplitude, phase and polarization state of a light wavefront can all be holographically recorded. Optical components including lenses and free space itself with their spatial transformation properties, as well as diffusers and spatial light modulators of phase, amplitude and polarization state, all enable controlled manipulation of light wavefront characteristics. The properties of light combined with the means for their control and recording are valuable tools for advanced security applications.

8.2 The counterfeit problem

Counterfeit goods constituted a global market of US$461 billion and accounted for around 2.5 percent of global imports in 2013 [1], up from an estimated 1.9 percent in 2008 [2]. The threats posed by counterfeit goods are not only economic but physical, in the form of dangerous medicines, equipment, spare parts, domestic appliances and toys.

It is widely accepted that in addressing such problems it is wise to employ overt, covert and tamper evident devices and forensic techniques. The choice of devices and methods depends on the scale of the threat and the consequences if it is not addressed. In this context it is apparent that some manufacturers appear to tolerate some volume of counterfeit product, particularly in cases where the end user is aware that the product is probably fake. In some markets however such compromise is clearly unacceptable where the health and safety of persons is at stake. Examples are pharmaceuticals, medicines, diagnostic instruments, food, animal feed and pharmaceuticals, spare parts for motor vehicles, ships and aircraft.

Regionally based pricing strategies give rise to authentic goods manufactured in low cost economies being made available in higher-cost economies. Although not in itself a threat to health or safety, such fraudulent activity implies weakness in the supply chain management system and may indicate the possibility of worse to follow. Only careful checks at each link in the chain by cross reference to a secure data base will help to alleviate the problem.

Verification is required for product authentication, brand protection and supply chain security as well as for documentation such as export/import licences, end user certificates, passports, driving licences, credit and debit cards, person identification, admission tickets and legal tender.

The growth in fake certification [3] demands thorough scrutiny of academic qualifications and specialised skills.

Contraband, narcotics, weapons and explosives are also of worldwide concern and rapid, effective means of detection are essential.

8.3 Holographic security and authentication

Since the mid-1960s, when fully 3-dimensional imaging by off-axis holographic methods was introduced [4], the idea of using recorded optical wavefronts for authentication has received much attention because of the large amount of information that can be carried. Wavelength, spatial distribution of amplitude and phase and polarization states may all be exploited for authentication purposes. The choice of which of the information bearing properties of light to use depends on the level of security required and cost.

8.4 Mass produced holograms

Mass produced holograms are usually made either in thin metallic foil or foil backed plastic or in a photopolymer, preferably one requiring no physical or chemical processing following the recording step. Other materials such as silver halide or dichromated gelatin may be used but these require chemical processing, with attendant financial and environmental costs. Such holograms are widely used on debit and credit cards and product packaging.

8.4.1 Rainbow holograms

The rainbow holography technique [5] enables one to make a hologram which can be viewed in ordinary, as opposed to laser light. A transmission hologram (H1) is made in the usual way (Fig. 8.1a) by recording the pattern of interference between two mutually coherent light beams one of which is reflected or scattered from some object.

Figure 8. 1

During reconstruction of the real image using the conjugate reference beam a horizontal slit aperture, S, is placed in contact with H1. If the original refence beam is collimated, it becomes its own conjugate by simply rotating the hologram in-plane through an angle of 180^0. A second hologram, H2, is recorded (Fig. 8.1b) and, using the original reference beam, a real orthoscopic image is obtained which can only be viewed through the reconstructed, conjugate image of the slit aperture, S*(Fig. 8.1c). In white light illumination of the

hologram the image is seen in different colours due to the dispersion effect of the slit (Fig. 8.1d). Horizontal perspective is maintained but vertical perspective is lost.

One can arrange matters so that the real image reconstructed from H1 is intersected by H2 (Fig. 8.2a) and a so-called image-plane hologram is then recorded.

Figure 8. 2

If H2 is recorded in photoresist, a surface relief hologram is formed which can then be electroplated with nickel to form a durable surface relief master hologram. This is used to make multiple copies by stamping in thin, high reflectivity metal foil or plastic backed by reflective foil so that the resulting copied holograms may be viewed in reflected light.

Such holograms are now ubiquitous but of questionable value for anti-counterfeit purposes as all those made from a single master are identical and fake holograms are easily produced. Even very crude versions of such holograms escape detection simply because they are not examined thoroughly, if at all. Considerable effort has been made to produce foil holograms which display increasingly complicated and interesting images, including images that change with viewpoint, to invite inspection. In addition, serial numbers have been ink printed or laser engraved underneath, beside or on the surface of the holograms.

Moiré techniques can provide additional security [6]. After recording the H2 hologram in the photoresist a grating pattern may also be recorded. The pattern in the form of a transparency is placed in contact with the photoresist and illuminated normally by an expanded laser (typically of wavelength 488 nm). The pattern is copied in surface relief in the developed photoresist. To authenticate a foil copy hologram made from the master, a second decoder transparency is placed on top of the copy and the moiré pattern observed in reflected light. A counterfeit hologram shows the wrong pattern or no pattern at all. A recorded surface relief pattern could however be characterised by phase contrast or optical scanning microscopy and subsequently incorporated in counterfeit holograms. To overcome this difficulty one may record the pattern as a hologram using an encrypted reference beam [7], see Section 8.7.1.

8.4.2 Volume reflection holograms

Volume reflection holograms [8] made by recording the interference pattern produced by overlapping, counter-propagating mutually coherent light beams (Fig. 8.3), can be viewed in white light since they also function as multi-layer, dielectric passband filters. The recorded fringe pattern is oriented approximately parallel to the hologram plane with spacing of $\lambda/(2n)$ where λ is the laser wavelength and n is the refractive index of the recording material. Unlike rainbow holograms there is no loss of vertical perspective.

Figure 8. 3

Increased image complexity can be achieved by using additional beams to illuminate the object from a range of angles of incidence to obtain a wider viewing perspective. Multiplexing using reference beams at different angles of incidence enables the display of quite different images when the hologram is illuminated from different directions. Mass production by contact copying from a high-quality master hologram, using low coherence

light, means that the same reconstructed image is visible in all of them. However, volume reflection holograms are not so easy to replicate as the information stored in them is distributed throughout the depth of the recording layer. For example, in a layer 30 μm thick there are typically 150 fringes of maximum brightness in an interference pattern recorded at 633 nm.

8.5 Serialised holography

The ideal hologram for anticounterfeiting applications is one that is unique to each individual product item or package, known as a serialised hologram. The hologram need not be particularly eye catching; what is important that it should display the data needed for authentication purposes. At the same time, it must be secure against the possibility of copying. If a hologram contains all of the information that is needed about the product which it accompanies then any data obtained from it must match that held in the manufacturer's database. The information provided by a hologram could be as minimal as the product manufacturer's name and logo but could also include a serial number, lot number, sell-by date if applicable, and place of manufacture. All this information can be encoded in a holographic quick response (QR) code if required.

One way to create a serialised hologram is to make use of the data to spatially modulate a beam of laser light so that it becomes the object beam in a hologram recording system. The data can be written onto a transmissive liquid crystal spatial light modulator (LCSLM) which can modulate both the phase and amplitude of a light wave front, or onto a liquid crystal on silicon (LCOS) phase only reflective SLM. The data is updated for each new serialised hologram that is to be recorded.

Production volumes of security holograms for packaging applications may run to many millions per year so that rapid recording without physical or chemical processing is essential, implying the need for a self-processing photopolymer. Production of serialised holograms of the type described has been pioneered by Optrace [9] an Irish start-up company, using machines which record up to 10,000 holograms per hour in a photopolymer developed by researchers in the Centre for Industrial and Engineering Optics at Dublin Institute of Technology [10].

Surface ablation by single 6 nS laser pulses has been used to record holographic surface gratings in well-ordered printed ink on a substrate, a process requiring a few minutes to complete [11] which may also enable mass production of serialised holograms.

8.6 Fourier methods for image comparison

The techniques discussed so far are all aimed at making holograms more difficult or even impossible to replicate by ensuring the uniqueness of the hologram itself. Holographic methods may also be used to compare images for authentication purposes by making use of the Fourier transform properties of lenses.

8.6.1 Optical matched filtering

Optical matched filtering by holographic means, also known as Vander Lugt filtering[12] or optical character recognition, has been extensively researched for security applications.

Starting with the definition of a 2-D spatial Fourier Transform $F(x_2, y_2)$ of a function $f(x_{1,}\, y_1)$

$$F(x_2, y_2) = \iint f(x_{1,}\, y_1) e^{\frac{jk(x_1x_2+y_1y_2)}{f}} dx_1\ dy_1 \qquad (8.\ 1)$$

A point source at $y_1 = b$ of unit amplitude in the front focal plane $(x_{1,}\, y_1)$ of a lens is specified by the delta function $\delta(y_1 - b)$ and has its Fourier transform $exp\ (-jkby_2/f)$ with $k = 2\pi/\lambda$ and λ the wavelength , in the back focal plane (x_2, y_2) (Fig. 8.4a).

Figure 8. 4

An optical character is written on transparency or a spatial light modulator and illuminated by laser light, coherent with the point source, to give complex amplitude $f(x_{1,}\, y_1)$. The combined intensity distribution in the back focal plane of the lens is

$$\left[exp\left(-\frac{jkby_2}{f}\right) + F(x_2, y_2)\right]\left[exp\left(\frac{jkby_2}{f}\right) + F^*(x_2, y_2)\right]$$

where $F^*(x_2, y_2)$ is the complex conjugate of $F(x_2, y_2)$.

This intensity distribution is recorded and subsequently illuminated by (Fig. 8.4 b) the Fourier transform of $g(x_{1,}\, y_1)$ to produce output

$$G(x_2, y_2)\left[exp\left(-\frac{jkby_2}{f}\right) + F(x_2, y_2)\right]\left[exp\left(\frac{jkby_2}{f}\right) + F^*(x_2, y_2)\right]$$

If $g(x_{1,}\, y_1)$ includes the character $f(x_{1,}\, y_1)$ at coordinates (p, q), i.e. $f(x_1 - p,\ y_1 - q)$ then $G(x_2, y_2)$ includes $F(x_2, y_2)\exp\,[-jk(px_2 + qy_2)]$

and $$G(x_2, y_2)\left[exp\left(-\frac{jkby_2}{f}\right) +\right]\left[exp\left(\frac{jkby_2}{f}\right) + F^*(x_2, y_2)\right]$$

includes $$|F(x_2, y_2)|^2\exp\,[-jk(px_2 + (q + b)y_2)/f]$$

which is a plane wavefront transformed by the second lens in Fig. 8.4b into a focussed point of light in its back focal plane at $x_3 = -p, y_3 = -(q + b)$ i.e. at the location of the character in the original input $g(x_{1,}\, y_1)$ which means that the procedure can determine the presence and the location of a character or group of characters in set of characters.

Each spatial frequency point must be located within an area determined by the resolution limit of the Fourier transform lens i.e. within $2.44\lambda f/D$ where D is the aperture diameter.

The procedure can be used to determine whether a given optical pattern such as a human fingerprint already exists in an optical data store of fingerprints, to protect against fraud or to verify the identities of persons.

The technique is invariant with respect to position but changes in scale or a rotation of the character constitute a different filter since the Fourier transform $F(x_2, y_2)$ is also rescaled and rotated. To overcome this difficulty the Fourier transform $F(x_2, y_2)$ can first be converted to polar coordinates $F(r, \theta)$ with $\theta = arctan(y_2/x_2)$ and $r = \sqrt{x_2^2 + y_2^2}$. Scale change then affects only r which *c*an be handled by a scale invariant 1-D Mellin

transform, which is a 1-D Fourier transform in $ln(r)$. Rotational invariance is effected by a 1-D Fourier transform in θ as this converts the rotations into phase factors which have no effect on the magnitude of the transformed output[13] [14]. To put it more simply a point $x_2 + jy_2$ in the Fourier plane is rewritten as

$$w = re^{j\theta} \tag{8. 2}$$

$$ln(w) = ln(r) + j\theta \tag{8. 3}$$

and change in scale by a factor β accompanied by a rotation through angle α in θ space gives

$$ln(w) = ln(r) + ln\ \beta + j\theta + j\ \alpha \tag{8. 4}$$

Equation 8.4 shows that separate 1-D Fourier transforms with respect to *ln*(*r)* and θ are invariant with respect to the now spatial shifts *ln*β and *j*α and the system is immune to rotations and scale changes of $f(x_{1,}\, y_1)$.

8.6.2 Joint transform correlation

In many security applications optical patterns can be directly compared for authentication purposes by joint transform correlation. Two patterns represented by complex amplitudes $f(x_1 - \frac{p}{2}, y_1 - \frac{q}{2})$ and $g(x_1 + \frac{p}{2}, y_1 + \frac{q}{2})$ in the front focal plane of a lens are illuminated by a collimated beam of laser light. Their Fourier transforms

$$F(x_2, y_2)\exp\left[-\frac{jk(x_2p+y_2q)}{2f}\right] \text{ and } G(x_2, y_2)\exp\left[\frac{jk(x_2p+y_2q)}{2f}\right]$$

interfere in the back focal plane and a recording is made of the interference pattern, having the form

$$I(x_2, y_2) = FG^*\exp\left[-\frac{jk(x_2p + y_2q)}{f}\right] + F^*G\exp\left[\frac{jk(x_2p + y_2q)}{f}\right] + |F|^2 + |G|^2 \tag{8. 5}$$

When the recording is illuminated the first term in Eq. 8.5 is transformed by the second lens in the 4*f* system of Fig. 8.4b and the correlation function

$$\iint f(x_3, y_3)g * (u - x_3 + p, v - y_3 + q)\, dudv$$

is obtained in the back focal plane *(x_3, y_3)* while the second term gives

$$\iint f * (u - x_3 - p, v - y_3 - q)g(x_3, y_3)\, dudv$$

The term $|F|^2 + |G|^2$ gives rise to a point of light at the focus of the second lens.

The correlation integral has maximum value if $f(x_{1,}\, y_1)$ and $g(x_{1,}\, y_1)$ are identical.

For real time applications, four wave mixing in a photorefractive medium [15] is used. Fourier transforms *F* and *G* of coherent spatial distributions of horizontally plane polarized light *f* and *g* are allowed to interfere with *H*, the Fourier transform of a third, vertically

polarized distribution, *h*, in the photorefractive medium (Fig. 8.5) and an output light signal *S* is obtained with

$$S \sim (FH^*)G$$

Figure 8. 5

If *F* is a plane wavefront produced by a point source at the focus of a lens, then

$$S \sim H^*G$$

which provides the correlation of *h* and *g* in the front focal (Fourier) plane of lens L_1.

Alternatively, if *G* is a plane wavefront, joint transform correlation between *f* and *h* is obtained since.

$$S \sim FH^*$$

8.7 Encryption methods in holography

In the holographic reconstruction process the object beam is reproduced by diffraction of the reference beam at the hologram. If the object beam is to be reconstructed accurately the correct reference beam must be used. This means that the wavelength and spatial distribution of phase in the reference beam must be the same as those used at the recording step. This requirement makes it possible to implement several hologram encryption methods.

8.7.1 Phase coded reference beam encryption

8.7.1.1 Random phase encoding

A diffuser in the path of the reference beam in holographic recording imposes a random spatial phase distribution on the reference beam [16] creating a speckled reference beam. The minimum size, σ, of the speckles at the hologram recording plane is given by

$$\sigma \cong \frac{\lambda l}{d} \qquad (8.\ 6)$$

where d is the diameter of the laser beam of wavelength λ, at the diffuser and l the distance between diffuser and recording plane [17]. Successful reconstruction requires the diffuser to be precisely relocated. An error in positioning resulting in speckle displacement of greater than σ results in speckle decorrelation and the corresponding holographic image will not be reconstructed.

Conventional ground glass diffusers can significantly reduce the optical power of the reference beam but holographic diffusers with greater than 85% transmissivity are available. Alternatively, a liquid crystal on silicon (LCOS) phase only spatial light modulator may be employed. Such devices with up to 4 million pixels and frame rate of tens of Hz allow rapid switching of the reference beam phase mask between hologram recordings. Again, reconstruction of the holographic image can only be successful if the correct phase mask is employed as a decryption key.

An additional encryption key can be added by specifying a virtual wavelength. It can be shown that even with the correct phase mask in place at reconstruction a deviation of 0.00002 nm from the specified wavelength means that the image cannot be decrypted [18].

In an extension of the random phase encoding technique [19] a key hologram, KH, is recorded using a diffuser as object. Then the conjugate image is reconstructed to serve as a reference beam with two converging object beams to record a security hologram (SH), see Fig. 8.6. If the security hologram is reconstructed using the wrong phase coded reference, then the focussed spots of light produced by lenses L1 and L2 do not appear. Security is further enhanced by recording two holograms of each converging object beam with a slight axial or transverse displacement of lenses L1 and L2 between exposures. On reconstruction, a concentric ring fringe pattern is seen in the case of axial translation or straight-line parallel fringes in the case of an in-plane translation as verification of the key hologram.

Figure 8. 6

8.7.1.2 Deterministic orthogonal phase coding

A form of deterministic phase coding, called orthogonal phase coding [20] offers significant advantages over the use of random diffusers as there are no mechanical parts in the system and no need for mechanical repositioning. The technique may be used to ensure secure storage of information in the form of data pages, each data page being recorded as a hologram.

A set of laser beams each having the same amplitude and phase φ, which is either *0* or π relative to the others, comprises the reference wave in a holographic recording set up and interferes in the recording medium, usually a photorefractive crystal, with a data page O_n, n an integer. The complete wavefront of the phase coded reference wave must interfere with the data page. To ensure that this is the case, the page is Fourier transformed and overlapped in the recording medium with the reference wave focussed so that it is discretized into its angular spectrum.

If *N* pages are to be recorded, there will be *N* phase coded reference beams and for each fresh data page, the set of reference beam phases is altered so that the complete holographic recording of the *N* data pages is given by

$$\left(\sum_{n=1}^{N} O_n\right)\left(\sum_{n=1}^{N}\sum_{m=1}^{N} exp(j\varphi_{n,m})\right)^{*} + \text{complex conjugate}, \quad n, m \text{ integers}$$

On reconstruction the holographic memory is illuminated by the phase coded reference beam

$$\sum_{m=1}^{N} exp(j\varphi_{k,m})$$

and the data page O_n is retrieved from the recorded set of N pages without crosstalk, provided that the phase codes are orthogonal.

$$\left(\sum_{m=1}^{N} exp(j\varphi_{k,m})\right) O_n \left(\sum_{n=1}^{N}\sum_{m=1}^{N} exp(j\varphi_{n,m})\right)^{*} = \begin{matrix} 0, k \neq n \\ 1 \end{matrix} \quad (8.7)$$

Equation 8.7 means that in order to retrieve a data page, one must use the phase coded reference beam with which it was recorded. The use of any other code produces zero output.

The appropriate orthogonal phase codes are obtained using the Walsh-Hadamard algorithm

$$H^{(0)} = 1, \qquad H^{(0)} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad H^{(p+1)} = \begin{bmatrix} H^{(p)} & H^{(p)} \\ H^{(p)} & -H^{(p)} \end{bmatrix} \quad (8.8)$$

where p is a positive integer. From Eq. 8.8 we obtain

$$H^{(2)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (8.9)$$

Zero phase shift is represented by 1 and a phase shift of π is represented by -1. For example, the second row of the matrix in Eq. 8.9 has phase code $0, \pi, 0, \pi$. Then, if we record a data page using a reference wave with this phase code and attempt to retrieve it using the phase code in the third row, we obtain zero output.

The use of binary phase codes based on Hadamard matrices means that the number of phase shifts is either just 2 or an even integer power of 2 so the SLM is not used very efficiently. The use of unitary matrices to implement phase coding makes more efficient use of the SLM [21].

8.7.2 Double random encryption

Double random encryption techniques for image security applications have been extensively studied in the Fourier [22] and Fractional Fourier domains (Section 8.6.3). The encrypted data can also be holographically recorded [23] using random or deterministic phase-coded reference beams.

An image $f(x_1, y_1)$ is multiplied by a phase mask in which phase is randomly distributed between *0* and 2π. The result

$$f(x_1, y_1)\exp\left[j2\pi n(x_1, y_1)\right]$$

where $n = RND[0,1]$, is convolved with an optical transfer function $h(x_1, y_1)$ whose Fourier transform is a constant amplitude, random phase function $\exp\left[j2\pi v(x_2, y_2)\right]$ giving encrypted output

$$\psi(x_1, y_1) = f(x_1, y_1) \exp[j2\pi n(x_1, y_1)] \otimes h(x_1, y_1) \quad (8.10)$$

which is holographically recorded. ($\otimes$ means convolution).

To decrypt the reconstructed image $\psi(x_1, y_1)$ is Fourier transformed then multiplied by $\exp[-j2\pi v(x_2, y_2)]$ and the result Fourier transformed again to give output

$$f(x_1, y_1) \exp[j2\pi n(x_1, y_1)]$$

A CMOS or other imaging device will provide output $|f(x_1, y_1)|^2$. A similar double encryption system involves first converting the input $f(x_1, y_1)$ into a phase only image [24] providing better performance.

8.7.3 Polarization encryption

In double random polarization encryption [25] a binary image is converted to a pixel array of orthogonal linear polarization states using an SLM so that the image is rendered visible only by means of a linear polarizer. Double encryption is by means of polarization modulation masks using SLMs at the input and Fourier planes. Each SLM imposes a random phase shift between the orthogonal polarizations at each pixel so that the output light from the pixel is in a random elliptical polarization state. Polarization holograms are recorded in bacteriorhodopsin by photoinduced anisotropy and are optimally reconstructed using counter-propagating, orthogonal circularly polarized beams (Fig. 8.7).

8.7.4 Fractional Fourier encryption

It has been pointed out [26] [27] that the propagation of light through a system of lenses is mathematically described by a continual process of fractional Fourier transformation, the amplitude and phase spatial distributions evolving through fractional transforms of increasing order.

A system of lenses placed between a planar, partially transparent object in the x, y plane and a hologram recording plane, can act as a fractional Fourier encryption key [28] whose parameters, *a, b* and α in the example shown in Fig. 8.7 are determined by the distances d_1, d_2, d_3 and d_4 and the focal lengths f_1 and f_2, all of which can be chosen arbitrarily.

Figure 8. 7

The fractional Fourier transform calculated in the intermediate plane x', y' (with y' dependence omitted for simplicity) is

$$g(x') = K \int f(x)\, e^{j\pi\left(\frac{a^2x^2 + b^2x'^2}{\tan\alpha} - \frac{2abx'x}{\sin\alpha}\right)} dx \quad (8.11)$$

Its parameters are given by

$$a^2 = \frac{\sqrt{f_1 - d_2}}{\lambda\sqrt{f_1 - d_1}[f_1^2 - (f_1 - d_1)(f_1 - d_2)]^{\frac{1}{2}}}$$

$$b^2 = a^2 \frac{f_1 - d_1}{f_1 - d_2}$$

$$\alpha = \cos^{-1} \sqrt{\frac{(f_1 - d_1)(f_1 - d_2)}{f_1}} \qquad (8.\ 12)$$

The fractional Fourier transform at the hologram plane is calculated from Eq. 8.11 with the parameters by *a, b* and α obtained by substituting d_3 for d_1, d_4 for d_2 and f_2 for f_1 in the parameter equations 8.12.

Reconstruction by the conjugate reference wave leads to the formation of a decrypted real image at the original location of the object, only if the fractional Fourier decryption key is applied, meaning that the light wave diffracted by the hologram at reconstruction must propagate through precisely the same optical system in reverse. Additional security may be provided by double encryption (Section 8.6.2), placing a random phase mask in contact with the input image and a second, statistically independent phase mask in the intermediate plane in Fig. 8.7. Knowledge of either the phase masks alone or of the fractional Fourier encryption key alone will not suffice to decrypt the image [29].

Additional lenses may be included in the optical system to make the encryption key more secure.

A virtual axial translation may be given to each of the pixels in the input image that is to be encrypted. The translation distance is unique to each pixel effectively converting the image into a 3-D object [30][31]. The spatial distribution of the translations, $d(x, y)$, is thus an additional encryption key.

8.7.5 Fresnel domain double random phase encryption

Double random phase encryption may be implemented in the Fresnel domain for added security [32]. Only the two phase masks are required. Lenses are not needed. The distances d_1 between the two phase masks, and d_2 between the second phase mask and the output plane of the doubly encrypted image, as well as the wavelength, may all be used for encryption purposes. The phase mask encryption keys alone are insufficient for decryption as Fresnel transformation determines the complex amplitude distributions in the planes of the phase masks and errors in d_1, d_2 or wavelength will cause decryption to fail. Decryption of the image requires reconstruction using the conjugate reference wave, or four wave mixing, with the phase masks in their original positions.

One of the most important features of techniques such as double random, fractional Fourier and Fresnel encryption is that the information may secured and decrypted by computational methods.

8.8 Digital holographic security

Digital holography using CCD or CMOS cameras as hologram recording devices, has led to the development of holographic microscopy as well as applications in metrology and

security. Here some phase-shift methods for digital recording of encrypted holograms and reconstructing the encrypted images, are described.

8.8.1 Phase shift digital holography

Phase shift methods are needed to obtain the encrypted image from the digital hologram. Phase shift digital holography normally requires the object and reference beams to be spatially separated in a Mach-Zehnder interferometer (Fig. 8.8) so the low spatial resolution of digital cameras (~100 lines mm^{-1}) requires that the beams are subsequently recombined onto a common propagation path before incidence on the CMOS sensor.

Figure 8. 8

There are several algorithms involving two or more phase shifts for obtaining the map of phase difference, $\emptyset_O - \emptyset_R$ between the object and reference waves. A reliable algorithm should have a high degree of immunity to deviation of a phase shift from its specified value [33] and should not necessarily require that the phase shifts be known. However, the greater the number of phase shifted holograms, the greater the computational burden associated with decryption and the channel capacity required for transmission over a communications network.

8.8.1.1 Two phase shifts

A collimated light beam is spatially modulated by a 2-D image mask in input plane (x_1, y_1) to give an object wave $o(x_1, y_1)$ which is then randomly phase modulated by a phase only SLM giving [34]

$$o(x_1, y_1)\exp\,[j\phi(x_1, y_1)]$$

This is Fourier transformed giving

$$O(x_2, y_2) = |O(x_2, y_2)|exp[j\emptyset_O(x_2, y_2)] \quad (8.\ 13)$$

in the plane (x_2, y_2) of the camera sensor. A collimated reference wave spatially modulated by a phase only SLM using random phase values of *0* and π, is also Fourier transformed to become

$$R(x_2, y_2) = |R(x_2, y_2)|exp[j\emptyset_R(x_2, y_2)] \quad (8.\ 14)$$

acting as an encryption key. A hologram $I(x_2, y_2)$ is recorded with

$$I(x_2, y_2) = |O(x_2, y_2)|^2 + |R(x_2, y_2)|^2 + 2|O(x_2, y_2)||R(x_2, y_2)|cos(\emptyset_O - \emptyset_R) \quad (8.\ 15)$$

A second hologram recorded with a phase shift of $\pi/2$ between the beams is given by

$$I'(x_2, y_2) = |O(x_2, y_2)|^2 + |R(x_2, y_2)|^2 + 2|O(x_2, y_2)||R(x_2, y_2)|sin(\emptyset_O - \emptyset_R) \quad (8.\ 16)$$

The D. C. terms $|O(x_2, y_2)|^2$ and $|R(x_2, y_2)|^2$ can be obtained separately and removed from the expressions for *I* and *I'* by alternately blocking the reference and object beams to obtain

$$J = |O(x_2, y_2)||R(x_2, y_2)|cos(\emptyset_O - \emptyset_R) \quad (8.\ 17)$$

$$J' = |O(x_2, y_2)||R(x_2, y_2)|sin(\emptyset_O - \emptyset_R) \quad (8.\ 18)$$

where $\emptyset_O - \emptyset_R = \tan^{-1}\left({}^{J'}/_{J}\right), \qquad |O(x_2, y_2)||R(x_2, y_2)| = \sqrt{J^2 + J'^2}$

from which we obtain

$$H(x_2, y_2) = |O(x_2, y_2)||R(x_2, y_2)| \exp[j(\emptyset_O - \emptyset_R)] \qquad (8.\ 19)$$

To decrypt the image, $H(x_2, y_2)$is multiplied by the encryption key $R(x_2, y_2)$

and the result divided by $|R(x_2, y_2)|^2$ giving

$$|O(x_2, y_2)| \exp[j\emptyset_O(x_2, y_2)]$$

which is inverse Fourier transformed and the modulus of the result $|o(x_1, y_1)|$ is the original input image.

Phase shift can be implemented by a piezoelectrically translated plane mirror in the path of the reference beam. Alternatively, as shown in Fig. 8.8, light which is plane polarised at 45° to the plane of the Mach-Zehnder interferometer is split between the two arms, the reference beam passing through a quarter wave plate whose fast axis is set normal to the interferometer plane. The beams are recombined at a second beamsplitter. A linear polariser with transmission axis normal to the interferometer plane allows interference between vertically plane polarised components of the object and reference waves. In-plane rotation of the linear polariser by 90° enables interference of the horizontally plane polarised components but with a phase shift of 90° between them.

8.8.1.2 Partitioned SLM

In a simpler approach a gray level image is first converted into ASCII form and multiplied by a random spatial phase mask in one part of a phase-only SLM (Fig. 8.9) located in the front focal plane of a lens and illuminated normally by a collimated laser beam [35]. The other part of the SLM is used to display a statistically independent, random phase pattern acting as a reference beam and encryption key. Two digital Fourier holograms with a phase shift of $\pi/2$ between them are recorded by a CCD or CMOS sensor in the back focal plane of a lens. To increase the dynamic range of the Fourier transform and thus make optimal use of the image sensor, a random phase mask is placed in contact with the SLM.

Figure 8. 9

The procedure is essentially as described in Section 8.8.1.1.

The SLM is partitioned so that gray levels are 8 - bit encoded clockwise into 3 x 3 arrays of pixels starting at the upper left pixel. A 128 x 128 input image thus occupies 384 x 384 pixels, the middle pixel in each 3 x 3 array being used for the reference beam. A disadvantage is that the ratio of object beam to reference beam intensity is as high as 8:1 but the object beam intensity range can be reduced to obtain a more favourable ratio.

8.8.1.3 Quadrature phase shift modulation

In quadrature phase shift keying (QPSK) modulation [36] one starts by ASCII encoding the binary gray level at each pixel of the image. A random phase mask is added. Quadrature

phase values are then assigned to each pair of binary digits starting with the MSB, for 8-bit gray level as follows

Binary	Phase
00	0
01	$\pi/2$
10	π
11	$3\pi/2$

Four pixels are needed for each image pixel with the phases written clockwise to a phase only SLM in the manner shown by the following examples

Gray level	ASCII	QPSK	
45	00101101	0	π
		$\pi/2$	$3\pi/2$
141	10001101	π	0
		$\pi/2$	$3\pi/2$

The phase image is recorded as a Fourier hologram. Reconstruction by the reference beam is followed by inverse Fourier transformation. Multiplication by the conjugate of the encryption phase map decrypts the original ASCII image.

8.9 Holography for imaging of concealed objects

The movement of contraband, chemical and biological weapons, firearms, explosives and narcotics within and across national boundaries is a matter of worldwide concern. Such items are usually concealed under optically opaque materials or in vehicle compartments lacking ease of rapid access, so the problem calls for the use of penetrating radiation usually in the millimetre and micrometre wavelength ranges. The competing demands for high spatial resolution and the ability to penetrate concealing materials favours the use of frequencies ranging from 300 to 1000 GHz [37].

The need for rapid acquisition of images suggests the use of a planar array of equally spaced detectors to record the interference pattern but such systems have low resolution, with a small field of view and are expensive. A reasonable compromise may be achieved by rapid scanning in the hologram plane using a single detector or a linear array of detectors scanning in one direction.

Direct detection methods use a vector network analyser (VNA) to measure both the amplitude and phase of the scattered radiation, relative to the amplitude and phase of the wave propagating directly from the transmitter and detected at a fixed location[38][39]. The scattered wave is detected at a number of points in the hologram plane. Thus, the

method allows one to obtain directly the spatial distribution of amplitude and phase of the wavefront scattered by the object. VNAs are rather expensive however.

Indirect recording of the complete interference pattern has been implemented by microwave heating of a cholesteric liquid crystal layer [40]. This produces changes in the colour of light reflected from the layer which can be photographed in monochrome to obtain a copy hologram from which the image is reconstructed using a visible laser. The sensitivity of the liquid crystal layer is rather low, at about 10mW cm^{-2}.

In another method [41] the illuminating radiation is phase locked to a local oscillator (LO). The receiver antenna is scanned over the hologram plane. The received signal is mixed with the LO to obtain an intermediate frequency which is low-pass filtered. The resulting voltage is proportional to the local phase of the received wave and modulates the intensity of a cathode ray tube light spot whose motion pattern is the same as that of the receiver. A photographic recording of the phase front of the wave scattered by the object, may be obtained, that is a phase only hologram.

In indirect methods the spatial pattern of intensity due to interference of the object and reference waves, is scanned in orthogonal directions in the hologram plane by an antenna connected to a detector, or along just one axis in that plane by a linear array of detectors. This method resembles the optical holographic method of Leith and Upatneiks [4] in that the phase difference between the radiation scattered by the object and that of the directly received reference radiation is encoded in the local spacing of an actual interference pattern.

Typically, the spatial Fourier transform of the recorded hologram is calculated and spatially filtered to extract the angular spectrum of the object wave. Recall that in optical off-axis holography one can use a plane reference wave incident at an angle θ to the normal at the hologram recording plane (x, y) so that the phase of the reference wave varies linearly along the x axis (say) of the hologram plane. However, at millimetre or micrometre wavelengths this is rather more difficult but the reference may be synthesized [42]. The output from a microwave transmitter of wavelength λ is split into two parts by a directional coupler. One part illuminates the object lying in a plane parallel to the hologram plane, at $z = -z'$, while the other is passed through a phase shifter and a variable attenuator to provide a synthesized reference signal of constant amplitude, which we will set at unity, and phase that is linearly dependant on position along the x axis of the hologram recording plane. Thus, the reference signal is given by $\exp(jkxsin\theta)$ where $k = 2\pi/\lambda$ and θ constant. The angular spatial frequency of this reference signal measured along the x axis is $2\pi sin\theta/\lambda$. A receiver antenna scans the hologram plane (x, y). The wave scattered by the object is $o(x, y)$ in the hologram plane and is mixed with the reference signal in a hybrid tee to provide an output proportional to the intensity of interference at each point of the scan.

The spatially dependant intensity is given by

$$I(x,y) = |o(x,y)|^2 + 1 + o^*(x,y)\exp(jkxsin\theta) + o(x,y)\exp(-jkxsin\theta) \qquad (8.\ 20)$$

Spatial Fourier transformation (*SFT*) gives the angular spatial frequency spectrum of $I(x,y)$ and, using the convolution theorem, one obtains

$$SFT[I(x,y)] = \left[O(k_x,k_y) \otimes O^*(k_x,k_y) + \delta(k_x)\right] + O^*(k_x,k_y) \otimes \delta(k_x - ksin\theta) + O(k_x,k_y) \otimes \exp(k_x + ksin\theta) \quad (8.\ 21)$$

The spectrum is shown in Fig. 8.10.

insert Fig. 8.10 here

The value of θ is chosen so that $sin\theta \geq 3k_{x_{max}}$ where $k_{x_{max}}$ is the maximum angular spatial frequency in the object wave, to ensure that the three terms in the angular spatial frequency spectrum (Eq. 8.20) do not overlap. A bandpass filter centred on spatial frequency $(ksin\theta, 0)$ is used to isolate $O(k_x,k_y)$, which is then spatial frequency shifted to centre on (0,0). The object wave in the hologram plane is obtained from the spatial Fourier transform of $O(k_x,k_y)$.

$$o(x,y) = \iint_{k_x,k_y} O(k_x,k_y)\, dk_x\, dk_y \quad (8.\ 22)$$

The angular spectrum of the object wave consists of a set of plane waves with propagation vectors $k_x, k_y, \sqrt{1-k_x^2-k_y^2}$ where $1 - k_x^2 - k_y^2 = k_z^2$, and the object wave in a plane (x,y) at $z = -z'$ is related to that at $z = 0$ by

$$O_{z=-z'}(x,y) = O_{z=0}\, exp(-jk_z z') = \iint_{k_x,k_y} O_{z=0}(k_x,k_y) exp\left[-j\left(k_x x + k_y y + k_z z'\right)\right] dk_x\, dk_y \quad (8.\ 23)$$

from which, by carrying out a spatial Fourier transform, a 2-D image of an object located at $z = -z'$ can be obtained. A 3-D image can be built up by calculating the object wave in a set of closely spaced planes normal to the *z*-axis, around the mid-plane of the object. The resolution along the *z*-axis is quite low unless a large area is scanned in the hologram plane. This method of image reconstruction is known as single frequency backward wave projection.

Wideband illumination enables the reconstruction of 3-D images rather than 2-D image slices [38]. The reflective properties of a 3-D object are described by the function $f(x,y,z)$. The response of a detector at x', y', Z_1 and at temporal angular frequency ω is

$$s(x',y',\omega) = \iiint f(x,y,z)\, e^{\{-2jk\sqrt{[(x-x')^2+(y-y')^2+(z-Z_1)^2]}}\, dxdydz \quad (8.\ 24)$$

where the amplitude of the transmitted wave is assumed constant and the receiver coincides with the transmitter.

The expression $e^{\{-2jk\sqrt{[(x-x')^2+(y-y')^2+(z-Z_1)^2]}}$ can be written

$$e^{\{-2jk\sqrt{[(x-x')^2+(y-y')^2+(z-Z_1)^2]}} = \iint e^{-j[k_{x'}(x-x')+k_{y'}(y-y')+k_z(z-Z')]}\, dk_{x'}dk_{y'} \quad (8.25)$$

The angular spatial frequencies $k_{x'}$ and $k_{y'}$ range from -2*k* to 2*k*.

From 8.24 and 8.25 we obtain

$$s(x', y', \omega) = \iint F(k_{x'}, k_{y'}, k_z) e^{j(k_{x'}x'+k_{y'}y'+k_zZ_1)} dk_{x'}dk_{y'} \quad (8.26)$$

where $F\left(k_{x'}, k_{y'}, k_z\right) = \left[\iiint f(x, y, z) e^{-j\left(k_{x'}x+k_{y'}y+k_zz\right)} dxdydz\right]$ is a 3-D spatial Fourier transform of $f(x, y, z)$.

Eq. 8.26 can be rewritten as

$$s(x', y', \omega) = IFT\left\{F(k_{x'}, k_{y'}, k_z) e^{jk_zZ_1}\right\} \quad (8.27)$$

Fourier transforming each side of Eq. 8.27 and removing the distinction between primed and unprimed coordinates gives

$$F\left(k_x, k_y, k_z\right) = FT_{2D}[s(x, y, \omega] e^{-jk_zZ_1} \quad (8.28)$$

We eliminate k_z since $k_x^2 + k_y^2 + k_z^2 = 4k^2$ and carry out an inverse transformation to form the image i.e.

$$f(x, y, z) = IFT_{3D}\left\{FT_{2D}\{s(x, y, \omega)\} \exp\left(-j\sqrt{4k^2 - k_x^2 - k_y^2}\, Z_1\right\}\right. \quad (8.29)$$

where $s(x, y, \omega)$ is the receiver response at x, y in the hologram plane, at temporal angular frequency ω, and Z_1 the distance between the transmitter/receiver and the x, y plane.

Because $s(x, y, \omega)$ is sampled at equal intervals in x, y and ω, resampling by linear interpolation is required at equal intervals of angular spatial frequency k_z.

Techniques that make use of both forward and backscattered radiation have also been implemented [43] and 3-D images have been obtained using single frequency radiation [44]

Finally an interesting application of the back propagation method has been reported [45]. The coherence of the radiation from 5GHz Wi-Fi router is exploited to record holograms over an area of 1 m^2. The router bandwidth of 70 MHz implies a coherence length of 4.3m. Reflections from walls create speckle but summing reconstructed images taken at a number of frequencies within the band helps to reduce its effect. A type of dark ground illumination is implemented to enhance the images. The technique may be exploited in tracking radiofrequency identification tags, 3-D motion capture and tracking for gaming and imaging though walls for security applications. It does however raise concerns about privacy and personal security.

References

[1] OECD/EUIPO, “Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact,” Paris, 2016.

[2] OECD, *The Economic Impact of Counterfeiting and Piracy*. 2008.

[3] H. Clifton, M. Chapman, and S. Cox, “‘Staggering’ trade in fake degrees revealed - BBC News,” 2018. [Online]. Available: https://www.bbc.com/news/uk-42579634. [Accessed: 11-Jun-2018].

[4] E. Leith and J. Upatneiks, “Wavefront Reconstruction with Diffuse Illumination and Three-Dimensional Objects,” *J. Opt. Soc. Am.*, vol. 54, no. 11, pp. 1295–1301, 1964.

[5] S. Benton, “Hologram Reconstructions with extended incoherent sources,” *J. Opt. Soc. Am.*, vol. 59, pp. 1545–6, 1969.

[6] X. Zhang, E. Dalsgaard, S. Liu, H. Lai, and J. Chen, “Concealed holographic coding for security applications by using a moiré technique.,” *Appl. Opt.*, vol. 36, no. 31, pp. 8096–7, 1997.

[7] A. K. Aggarwal, S. K. Kaura, D. P. Chhachhia, and A. K. Sharma, “Concealed moiré pattern encoded security holograms readable by a key hologram,” *Opt. Laser Technol.*, vol. 38, no. 2, pp. 117–121, 2006.

[8] Yu. N. Denisyuk, “Photographic reconstruction of the optical properties of an object in its own scattered radiation field,” *Sov. Phys. Dokl.*, vol. 7, p. 543, 1962.

[9] V. Toal and et al., “Serialised holography for brand protection and authentication,” *Appl. Opt.*, vol. xx, no. xx, pp. xxxx–x, 2018.

[10] I. Naydenova, H. Sherif, S. Martin, R. Jallapuram, and V. Toal, “US Patent 8,535,853 B2,” 2013.

[11] F. D. C. Vasconcellos *et al.*, “Printable Surface Holograms via Laser Ablation,” *ACS Photonics*, vol. 1, no. 6, pp. 489–495, 2014.

[12] A. B. Vander Lugt, “Signal detection by complex spatial filtering,” *Information Theory, IEEE Transactions on*. 1964.

[13] D. Casasent and D. Psaltis, “Position, rotation, and scale invariant optical correlation.,” *Appl. Opt.*, vol. 15, no. 7, pp. 1795–1799, 1976.

[14] P. Bone, R. Young, and C. Chatwin, “Position-, rotation-, scale-, and orientation-invariant multiple object recognition from cluttered scenes,” *Opt. Eng.*, vol. 45, no. 7, pp. 077203-8, 2006.

[15] D. Vacar, A. J. Heeger, B. Volodin, B. Kippelen, and N. Peyghambarian, “Compact, low power polymer-based optical correlator,” *Rev. Sci. Instrum.*, vol. 68, no. 2, p. 1119, 1997.

[16] A. M. Darskii and V. Markov, “Shift selectivity of holograms with a reference speckle wave,” *Opt. Spectoskopy*, vol. 65, pp. 392–5, 1988.

[17] C. Dainty ed., *Laser speckle and related phenomena*. 1984.

[18] X. Peng, L. Yu, and L. Cai, “Double-lock for image encryption with virtual optical wavelength.,” *Opt. Express*, vol. 10, no. 1, pp. 41–45, 2002.

[19] A. K. Aggarwal, S. K. Kaura, D. P. Chhachhia, and A. K. Sharma, “Encoded reference wave security holograms with enhanced features,” *J. Opt. A Pure Appl. Opt.*, vol. 6, no. 2, pp. 278–281, 2004.

[20] C. Denz, K. O. Müller, T. Heimann, and T. Tschudi, “Volume holographic storage demonstrator based on phase-coded multiplexing,” *IEEE J. Sel. Top. Quantum Electron.*, 1998.

[21] X. Zhang, “Unitary matrices for phase-coded holographic memories,” *Opt. Lett.*, vol. 31, no. 8, pp. 1047–9, 2006.

[22] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, vol. 20, no. 7, p. 767, 1995.

[23] B. Javidi, G. Zhang, and J. Li, “Encrypted optical memory using double-random phase encoding,” *Appl. Opt.*, vol. 36, no. 5, pp. 1054–8, 1997.

[24] N. Towghi, B. Javidi, and Z. Luo, “Fully phase encrypted image processor,” *J. Opt. Soc. Am. A*, vol. 16, no. 8, p. 1915, 1999.

[25] O. Matoba and B. Javidi, “Secure holographic memory by double-random polarization encryption.,” *Appl. Opt.*, vol. 43, no. 14, pp. 2915–2919, 2004.

[26] H. M. Ozaktas and D. Mendlovic, “Fractional Fourier optics,” *J. Opt. Soc. Am. A*, vol. 12, no. 4, p. 743, 1995.

[27] H. M. Ozaktas and D. Mendlovic, “Every Fourier optical system is equivalent to consecutive fractional-Fourier-domain filtering,” *Appl. Opt.*, vol. 35, no. 17, pp. 3167–3170, 1996.

[28] Y. S. Zeng, Y. K. Guo, F. H. Gao, and J. H. Zhu, “Principle and application of multiple fractional Fourier transform holography,” *Opt. Commun.*, vol. 215, no. 1–3, pp. 53–59, 2003.

[29] X. Wang, D. Zhao, and L. Chen, “Image encryption based on extended fractional Fourier transform and digital holography technique,” *Opt. Commun.*, vol. 260, no. 2, pp. 449–453, 2006.

[30] W. Chen and X. Chen, “Space-based optical image encryption,” *Opt. Express*, vol. 18, no. 26, pp. 1575–1577, 2010.

[31] C. Lin, X. Shen, and B. Li, “Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code,” *Opt. Express*, vol. 22, no. 17, p. 20727, 2014.

[32] G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” vol. 29, no. 14, pp. 1584–1586, 2004.

[33] J. Li *et al.*, “An advanced phase retrieval algorithm in N-step phase-shifting interferometry with unknown phase shifts,” *Sci. Rep.*, vol. 7, no. March, pp. 1–12, 2017.

[34] S. K. Gil, “2-Step Quadrature Phase-Shifting Digital Holographic Optical Encryption Using Orthogonal Polarization and Error Analysis,” *J. Opt. Soc. Korea*, vol. 16, no. 4, pp. 354–364, 2012.

[35] S. H. Jeon, Y. G. Hwang, and S. K. Gil, “Optical encryption of gray-level image using on-axis and 2-f digital holography with two-step phase-shifting method,” *Opt. Rev.*, vol. 15, no. 4, pp. 181–186, 2008.

[36] S. H. Jeon and S. K. Gil, “QPSK modulation based optical image cryptosystem using phase-shifting digital holography,” *J. Opt. Soc. Korea*, vol. 14, no. 2, pp. 97–103, 2010.

[37] D. M. Sheen, D. L. McMakin, J. Barber, T. E. Hall, and R. H. Severtsen, “Active imaging at 350 GHz for security applications,” *Proc. SPIE*, vol. 6948, no. March 2015, p. 69480M–69480M–10, 2008.

[38] D. M. Sheen, D. L. McMakin, and T. E. Hall, “Three-dimensional millimeter-wave imaging for concealed weapon detection,” *IEEE Trans. Microw. Theory Tech.*, vol. 49, no. 9, pp. 1581–1592, 2001.

[39] D. M. Sheen, D. McMakin, and T. E. Hall, “Near-field 3-dimensional radar imaging techniques and applications,” *Appl. Opt.*, vol. 49, no. 19, pp. E83–E93, 2010.

[40] C. F. Augustine, C. Deutsch, D. Fritzler, and E. Marom, “Microwave holography using liquid crystal detectors,” *Proc. IEEE*, vol. 57, p. 1333, 1969.

[41] N. H. Farhat and W. R. Guard, “Millimeter Wave Hologrphic Imaging of Concealed Weapons,” *Proc. IEEE*, no. September, pp. 1383–4, 1971.

[42] D. Smith, M. Elsdon, M. Leach, M. Fernando, and S. J. Foti, “3D Microwave imaging for medical and security applications,” *2006 Int. RF Microw. Conf. Proc.*, vol. 00, no. 4, pp. 233–237, 2006.

[43] R. K. Amineh, M. Ravan, A. Khalatour, and N. K. Nikolova, “3-D Near-field microwave holography using reflected and transmitted signals,” *IEEE Tranactions Antennas Propag.*, vol. 59, no. 12, pp. 4777–89, 2011.

[44] R. K. Amineh, M. Ravan, R. Sharma, and S. Baua, “Three-Dimensional Holographic Imaging Using Single Frequency Microwave Data,” *Int. J. Antennas Propag.*, 2018.

[45] P. M. Holl and F. Reinhard, “Holography of Wi-fi Radiation,” *Phys. Rev. Lett.*, vol. 118, pp. 183901-01 183901-05, 2017.