Compression of Optically Encrypted Digital Holograms Using Artificial Neural Networks

Alison E. Shortt, Thomas J. Naughton, and Bahram Javidi, *Fellow, IEEE*

***Abstract*—Compression and encryption/decryption are necessary for secure and efficient storage and transmission of image data. Optical encryption, as a promising application of display devices, takes advantage of both the massive parallelism inherent in optical systems and the flexibility offered by digital electronics. We encrypt real-world three-dimensional (3D) objects, captured using phase-shift interferometry, by combining a phase mask and Fresnel propagation. Compression is achieved by nonuniformly quantizing the complex-valued encrypted digital holograms using an artificial neural network. Decryption is performed by displaying the encrypted hologram and phase mask in an identical configuration. We achieved good quality decryption and reconstruction of 3D objects with as few as 2 bits in each real and imaginary value of the encrypted data.**

***Index Terms*—Artificial neural network (ANN), digital holography, image compression, optical encryption, three-dimensional (3D) image processing.**

I. Introduction

An important aspect of security and defense is information gathering, dissemination, processing, and analysis. Central to this is the encryption and decryption of messages for storage and transmission. Although public key cryptosystems are currently the state of the art, there is a place for private key systems in cases where hardware implementation permits very high throughputs. Optical implementation [1]–[14] is one such private key candidate that promises huge throughputs and is a promising application of display devices. Optics has some very promising scalability advantages over purely electronic systems as, in principle, the size of the key can be increased without increasing the encryption or decryption time.

Whereas conventional digital encryption algorithms transform a bit stream into a bit stream, almost all optical encryption systems transform an image into an image. When one is dealing with images, it is natural to consider compression. In fact, images rarely, if ever, are stored or transmitted without compression. This is because images, unlike text, often contain significant redundancy (motivating lossless compression) and contain minute details that might not be perceived by the human eye (motivating lossy compression). Analog optical implementations are also inherently error prone (nonlinear device responses, quantization, and finite-aperture optical elements) and are often designed to be robust to a certain amount of defects. We claim, therefore, that there is sufficient motivation to study compression, and quantization compression errors, in the context of optical image encryption. We only consider the application of compression after encryption (rather than the other way around) as the gross properties of optically encrypted images would seem to be similar regardless of the quantization levels or spatial distributions of the inputs.

Digital holography [15]–[21], and particularly phase-shift interferometry (PSI) [19]–[21], can record high quality representations of both the amplitude and phase of complex-valued optical wavefronts, and has been proposed for 3D object recognition and 3D display applications [22]–[25]. Recently, digital holography has been used in the encryption of two-dimensional (2D) images [6]–[8] and 3D objects [12]–[14].

In this paper, the complex-valued encrypted holographic pixels are quantized nonuniformly using an unsupervised artificial neural network (unsupervised ANN) to achieve lossy data compression. Two important differences between digital hologram compression and conventional image compression are that our holograms store 3D information in complex-valued pixels, and their inherent speckle content which gives the holograms a white-noise appearance. Holographic speckle is difficult to remove since it actually carries 3D information. Its presence causes lossless data compression techniques to perform badly, therefore lossy compression techniques are necessary for effective compression of 3D digital holograms [24].

Quantization in holograms [26], [27], and compression of real-valued [28] and complex-valued [13], [24], [25], [29]–[33], [35]–[37] digital holograms has received some attention to date. Some studies have also been performed on the decrypted-domain effects of perturbations, including quantization, in the encrypted domain [38], [39]. This introduces a third reason why compression of digital holograms differs to compression of digital images; a change locally in a digital hologram will, in theory, effect the whole reconstructed object. Furthermore, when gauging the errors introduced by lossy compression, we are not directly interested in the defects in the hologram itself, only how compression noise effects the quality of reconstructions of the compressed 3D object.

We used PSI to create our in-line digital holograms [22], [23]. These holograms were encrypted by perturbing the Fresnel diffraction of the 3D objects with a random phase mask. We simulated this encryption step in software [14]. The dimensions of each encrypted hologram are 1024×1024 pixels. Encrypted

Manuscript received March 30, 2006; revised June 22, 2006. The work of A. E. Shortt was supported by Enterprise Ireland and Science Foundation Ireland.

A. E. Shortt is with the Department of Computer Science, National University of Ireland, Maynooth, County Kildare, Ireland, and also with the Electrical & Computer Engineering Department, University of Connecticut, Storrs, CT 06269-2157 USA (e-mail: ashortt@cs.nuim.ie; Alison@engr.uconn.edu).

T. J. Naughton is with the Department of Computer Science, National University of Ireland, Maynooth, County Kildare, Ireland (e-mail: tom.naughton@nuim.ie).

B. Javidi is with the Electrical & Computer Engineering Department, University of Connecticut, Storrs, CT 06269-2157 USA (email: bahram@engr.uconn.edu).

Digital Object Identifier 10.1109/JDT.2006.884693

digital holograms have been successfully quantized previously. We extend these results [13] by choosing nonuniform distributions of quantization values. We describe these nonuniform quantization techniques and present experimental results to justify our final choice of a Kohonen competitive neural network. We consider each complex-value as a vector of length two and use the unsupervised ANN to locate the most suitable clusters in the encrypted digital hologram data. We then quantize our encrypted holograms with the centers of these clusters. We use a reconstructed-object-plane rms metric to quantify the quality of our decompressed and decrypted holograms.

In Section II, we outline how we perform encryption of the Fresnel propagation of 3D objects using a random phase mask, and how the complex wavefront is subsequently captured using PSI. The decryption and reconstruction steps are explained in Section III. We examine the amenability of encrypted digital holograms to lossless compression using four well-known techniques in Section IV. We discuss two types of Kohonen ANN that we used to quantize our 3D digital hologram data in Section V. We assess the performance of the nonuniform quantization techniques in Section VI and find one that best suits our hologram data. We then apply this lossy technique of quantization to the real and imaginary encrypted components of each holographic pixel in Section VII. In this section too, we quantify quantization error by measuring deformation in the decrypted and reconstructed 3D object intensities, and finally conclude in Section VIII.

II. Digital Hologram Encryption

The encrypted complex-valued holograms can be captured using an optical setup (shown in Fig. 1) based on a Mach-Zehnder interferometer architecture [22], [23]. A linearly polarized Argon ion (514.5 nm) laser beam is divided into object and reference beams, both of which are spatially filtered and expanded. The first beam illuminates the 3D object placed at an approximate distance $d_1 + d_2 = 350$ mm from a 10-bit 2028×2044 pixel Kodak Megaplus CCD camera. A random phase mask is placed a distance d_1 from the 3D object. Due to free-space propagation, and under the Fresnel approximation [40], [41], the signal at the detector plane $H_{\mathrm{E}}(x, y)$ is given by the superposition integral

$$H_{\mathrm{E}}(x,y) = \frac{-\mathrm{i}}{\lambda d_2} \exp\left(\mathrm{i}\frac{2\pi}{\lambda} d_2\right) \int\int_{-\infty}^{\infty} \exp\left[\mathrm{i}\Phi(x',y')\right] \times A_{\mathrm{M}}(x',y') \exp\left[\mathrm{i}\phi_{\mathrm{M}}(x',y')\right] \times \exp\left\{\mathrm{i}\frac{\pi}{\lambda d_2}\left[(x-x')^2 + (y-y')^2\right]\right\} \mathrm{d}x'\mathrm{d}y' \tag{1}$$

where A_{M} and ϕ_{M} are the amplitude and phase, respectively, of the signal in the plane of, but immediately before, the random phase mask Φ. $H_{\mathrm{E}}(x, y)$ will have both its amplitude and phase modulated by the mask and will have a dynamic range suitable for capture by a CCD camera. The reference beam passes through half-wave plate RP_1 and quarter-wave plate RP_2. This linearly polarized beam can be phase-modulated by rotating the two retardation plates. Through permutation of the fast and slow axes of the plates we can achieve phase shifts of 0, $-\pi/2$, $-\pi$, and $-3\pi/2$. The reference beam combines with the light diffracted from the object and forms an interference pattern in the plane of the camera. At each of the four phase shifts we record an interferogram. Using these four real-valued images, the complex camera-plane wavefront can be approximated to good accuracy using PSI [22], [23].

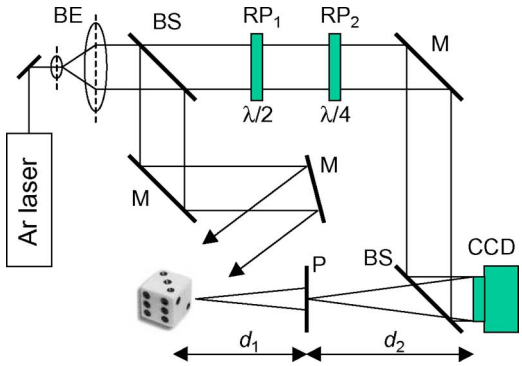

Fig. 1. Experimental setup for 3D object encryption using phase-shift digital holography: BE, beam expander; BS, beam splitter; M, mirror; RP, retardation plate; P, phase mask. (Color version available online at http://ieeexplore.ieee.org.)

In this system, the encryption key is $(\Phi, x, y, d_2, \lambda, e_{\mathrm{x}}, e_{\mathrm{y}}, d_1)$, consisting of the random phase mask, its position in 3D space, the wavelength of the illumination, the dimensions of the detector elements (for a pixilated device), and the distance between the mask and the notional center of the object, respectively. This key is also exactly the decryption key: a means of decrypting and reconstructing an arbitrary view of the 3D object encoded in the hologram.

III. Decryption and Reconstruction

The decryption and reconstruction of the digital hologram can be carried out optically or digitally. The hologram is propagated a distance d_2 to plane $P$and decrypted by multiplying it with the phase mask. It is reconstructed through further Fresnel propagation to focus in any chosen plane in the range $d_1 \pm D$.

A decrypted digital hologram contains sufficient amplitude and phase information to reconstruct the complex field $U(x, y, z)$ in a plane in the object beam at any distance z from the camera. Like traditional holography [41], different angles of view of the object can be reconstructed using different windowed subsets of the hologram. These views are obtained by multiplying the decrypted and reconstructed object by a suitable linear phase factor [22] within the angular range of the hologram. The number of possible viewing angles is dependent on the ratio of the window size to the full charge-coupled device (CCD) sensor dimensions. Our CCD sensor is approximately 18.5 mm $\times$ 18.5 mm and so a 1024×1024 pixel window has a maximum lateral shift of 9 mm across the face of the CCD sensor [23]. So the range of viewing angles that are possible with an object placed $d = 350$ mm from the camera is ± 0.74 deg. Smaller windows will permit a larger range of viewing angles at the expense of image quality at each viewpoint.

The intensity images of two of the objects used in our experiments are shown in Fig. 2(a) and (b). These images were reconstructed from digital holograms that were created using a similar setup to that shown in Fig. 1, without the phase mask

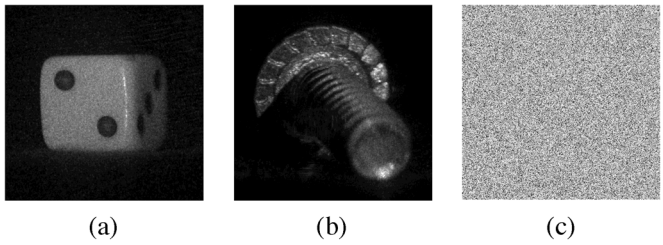

Fig. 2. Objects used in the study. (a) Die. (b) Bolt. (c) Example of a random phase mask.

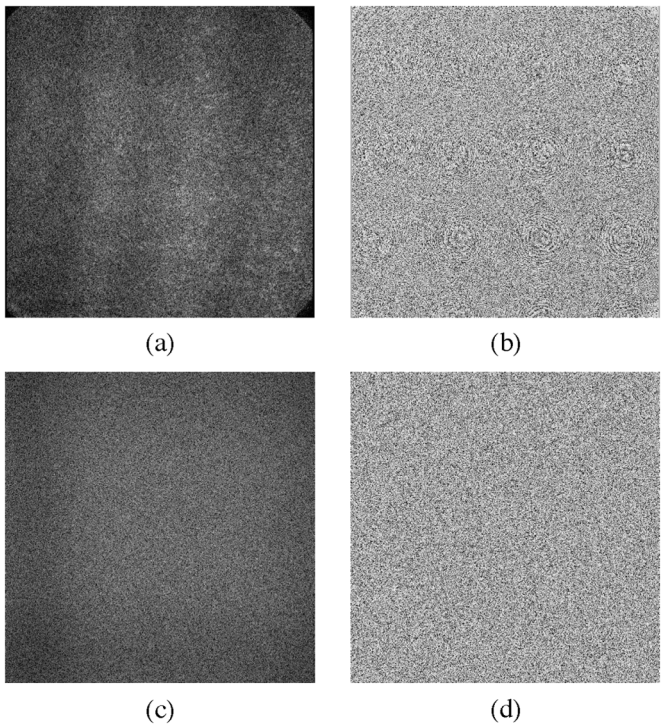

Fig. 3. Bolt before and after encryption. (a) Amplitude and (b) phase of original hologram. (c) Amplitude and (d) phase of encrypted hologram.

positioned in plane P[22], [23]. Both objects are approximately 5 mm $\times$ 5 mm $\times$ 5 mm in size and were positioned 323 mm (for the die) and 390 mm (for the bolt) from the camera.

By digitally encrypting the holograms that were captured without a random phase mask [14], we achieve added flexibility and security [14], while still accommodating the possibility for a real-time optical reconstruction [9], [25]. Fig. 2(c) shows the 1024 $\times$ 1024 pixel phase mask used in our experiments. It contains values chosen with uniform probability from the range $[0, 2\pi)$ using a pseudorandom number generator. The position of the phase mask is illustrated in Fig. 1 and the ratio of the distances $d_1 : d_2$ is 35:65. In Fig. 3 we show the amplitude and phase of the bolt hologram before encryption, and after encryption as described by (1). In Fig. 4 we show the results of reconstructing an encrypted digital hologram with and without the phase mask used in the encryption step.

IV. Lossless Compression of Encrypted Digital Holograms

In order to motivate the need for lossy compression techniques, the digital holograms were treated as binary data

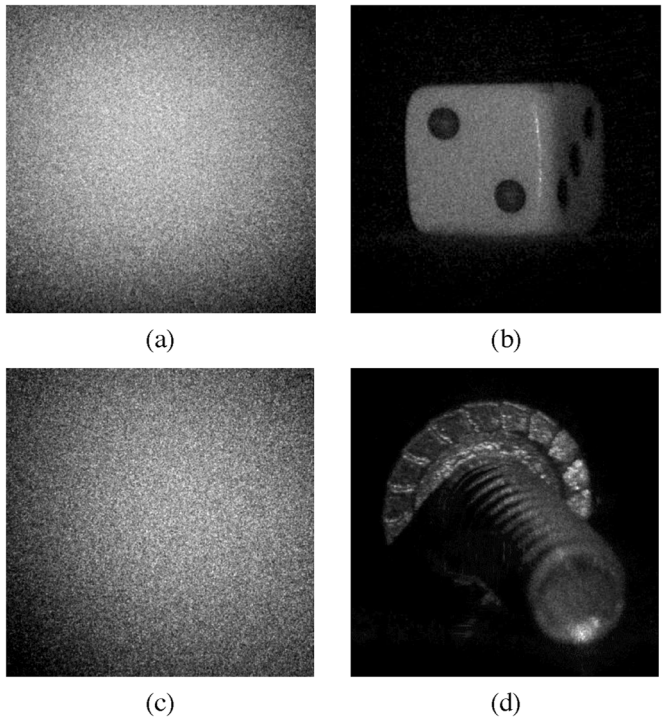

Fig. 4. Reconstruction of die (a) without and (b) with phase mask. Reconstruction of bolt (c) without and (d) with phase mask.

streams and compressed using the lossless data compression techniques of Huffman [42], Lempel-Ziv (LZ77) [43], Lempel-Ziv-Welch (LZW) [44], and Burrows-Wheeler (BW) [45]. Huffman coding, an entropy-based technique, is one of the oldest and most widely used compression methods. Each symbol in the input is replaced by a codeword, with more frequent symbols assigned shorter codewords. The LZ77 algorithm takes advantage of repeated substrings in the input data and replaces variable length strings with a pointer to the previous occurrence of that string. LZW improves upon LZ77 by maintaining a lookup table of variable sized codewords and is also less biased towards local redundancy. Finally, the BW technique uses a sorting operation to transform its input into a format that can be compressed very effectively using standard techniques (in our particular implementation, Huffman coding). The two digital holograms used in the experiments have dimensions of 1024 $\times$ 1024 pixels, and in their native MATLAB format each complex-valued pixel is represented as two 8-byte floating point values. In a previous study of unencrypted digital holograms [24], lossless techniques have been shown to achieve compression ratios in the range [1.0,6.66] where compression ratio is calculated by dividing a hologram's uncompressed size by its compressed size.

The two holograms were encrypted with the phase mask shown in Fig. 2(c). For these experiments, unencrypted holograms of the 3D objects were captured optically [22], [23] and the encryption steps described in (1) were simulated in software [14]. The four lossless compression techniques were applied to each hologram and the results are shown in Table I. The poor compression ratios testify to the lack of redundancy and structure in the encrypted hologram data, even compared to unencrypted digital holograms. The random phase mask,

TABLE I
LOSSLESS COMPRESSION OF ENCRYPTED HOLOGRAMS; C.R., COMPRESSION RATIO

Hologram	Size (kB)	LZ77 (kB)	LZW (kB)	Huff. (kB)	BW (kB)	LZ77 c.r	LZW c.r.	Huff. c.r.	BW c.r.
die	4097	3918	5296	3914	4003	1.05	1.00	1.05	1.02
bolt	4097	3918	5297	3915	4003	1.05	1.00	1.05	1.02
Averages:						1.05	1.00	1.05	1.02

combined with Fresnel propagation, is very effective at removing apparent structure from the hologram data. These results illustrate the urgent need to explore lossy compression techniques suitable for encrypted digital holograms. One such lossy technique that has been successfully applied to encrypted digital holograms is uniform quantization of individual complex amplitudes [13], motivated by the lack of correlation between neighboring pixels. However, there is some structure in that there is correlation between the real and imaginary components in each pixel [35] and this structure is not exploited with a uniform quantization technique. This is the motivation for a nonuniform quantization approach.

V. ANNs SUITABLE FOR NONUNIFORM QUANTIZATION

ANN clustering algorithms have been successfully used for vector quantization, image compression, and speech compression [46]–[53] in the past. We previously found that there was correlation between the real and imaginary components of the complex-valued pixels in our digital holograms [35]. In order to exploit this natural correlation, each complex-valued pixel can be regarded as a vector of length two and vector quantization techniques can be applied to our encrypted data. We use the Kohonen competitive network [54] (also known as a vector quantization network) and the self-organizing map (SOM) [54] for quantizing our digital holograms.

The Kohonen competitive neural network [54] consists of two-layers: an input layer and a competitive layer. Weight vectors, connecting the input neurons to the output neurons, are initially set to the midpoint of the range of input values. An unsupervised learning strategy is used to update the weights, W, at time $t+1$, as [55]

$$W(t+1) = W(t) + \alpha(t)\left[x(t) - W(t)\right]) \tag{2}$$

where α is the learning rate, and x is the input vector. This allows these weight vectors to learn to cluster the input data naturally without any *a priori* information. An input vector is randomly chosen and presented to the network. The neuron whose weight vector is closest to the input vector wins the competition and has its weight vectors updated in order to draw it closer to the input vector and the weight vectors of all other neurons are unchanged. This is known as hard competition.

Kohonen desired a characteristic known as equiprobability for his competitive network, whereby an input vector chosen at random from the training set would have equal probability of being close to any of the weight vectors. It was Desieno who proposed a conscience mechanism that not only enforced equiprobability but also fixed the over-clustering problem (the problem of combining a number of diverse clusters into one large cluster) and alleviated the dead neuron problem (where neurons that are positioned far away from the input data may never influence clustering) that were present in the original competitive network. By monitoring the success of all neurons, conscience creates a fatigue effect [54] on neurons that are winning a lot in order to give others a chance. This encourages neurons to spread out into undersampled areas of the input space. This network also has a learning rate associated with it that controls the amount by which the winning weight vectors are updated during learning. Training ceases when the maximum number of epochs is reached, performance has minimized the goal, or the maximum amount of time has been exceeded.

The SOM [54], differs from the Kohonen competitive network in that it updates both the winning neurons weights and the weights of neurons located in the neighborhood of the winner. This is known as soft competition and the weights, W, at time $t+1$ are updated as [55]

$$W(t+1) = W(t) + h(t)\left[x(t) - W(t)\right] \tag{3}$$

where $x(t)$ is the input neuron, and $h(t)$ is calculated as [55]

$$h = \alpha(t)\exp\frac{-|r_i - r_c|^2}{\sigma^2} \tag{4}$$

where α is the learning rate, r_i and r_j are the positions of neurons i and j, and σ is decreased slowly over time. The neighboring weight vectors are updated to a lesser degree depending on how far away from the winning neuron they are. Experimentation has shown that the best results are obtained when the neighborhood is large initially and shrinks monotonically over time [54]. This results in a rough global ordering of the input data initially and as the neighborhood shrinks this ordering becomes finely tuned. The SOM network also has a two-layer structure. The competitive layer consists of a grid, usually two-dimensional, of connected neurons. This grid stretches and mutates its shape to arrange its neurons to successfully represent the patterns in the input data. The number of neurons in the grid affects quality of results and training time; more neurons give improved accuracy but increase training time.

During the ordering learning phase of the SOM, the neighborhoods are defined, i.e. neurons arrange themselves so that neurons that are sensitive to similar inputs will be located close together. The learning rate is initially high to allow self-organization. In the tuning phase, the weight vectors are expected to spread out relatively evenly over the input space, while retaining their topological ordering that was found during the ordering phase. This tuning phase generally performs between 10 to 100 times as many steps as the ordering phase [54]. The learning rate should be kept small as the neighborhood will also be small at this stage. The distance function most often used for the SOM is Euclidean distance.

Both the Kohonen competitive and the SOM neural networks are given an initial number of cluster centers and will use as many as required to successfully cluster the input data. A maximum number of epochs is also allocated. Both networks learn

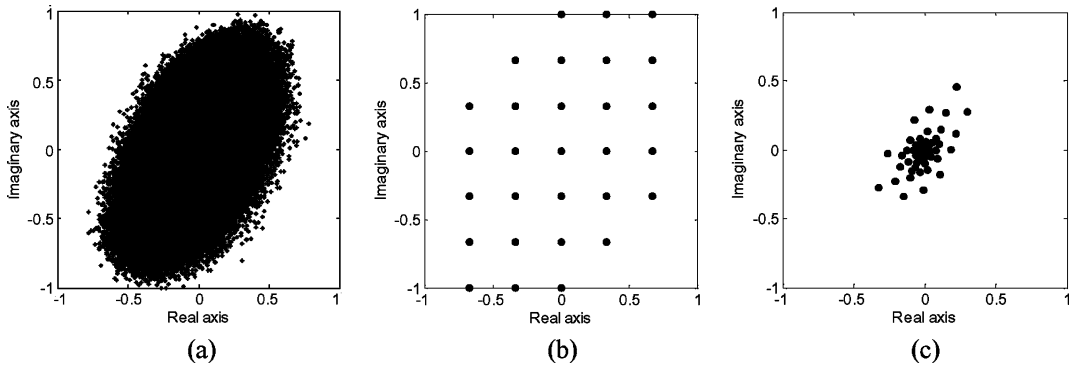

Fig. 5. Scatter plots of data in die: (a) before quantization, (b) uniformly quantized with 49 clusters, (c) k-means quantization with 49 clusters.

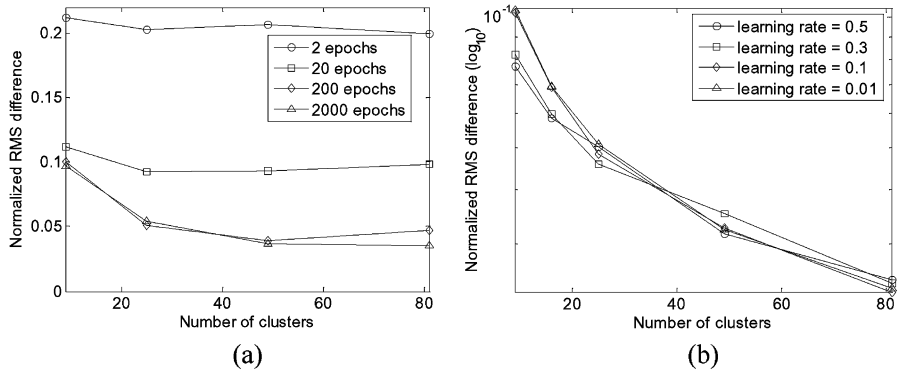

Fig. 6. Results of experiments (a) using a 32 × 32 pixel window of die to determine required number of epochs and (b) using a 128 × 128 pixel window of die to determine required learning rates. Both for Kohonen competitive.

the distribution of the input data. In addition to this, SOM learns and preserves the structure of the input space; neighboring neurons represent similar input data and densely populated regions are mapped to larger regions in the output space. In the next section we discuss the results we obtained from evaluating these neural network quantization techniques with our digital hologram data.

VI. Evaluation of Nonuniform Quantization Techniques

Uniform quantization is the optimal choice when the data values are uniformly distributed. Since our hologram data consists of unevenly distributed complex values [see Fig. 5(a)], nonuniform quantization techniques are more suitable.

Initially we looked at the popular k-means clustering algorithm [56], which is suitable for clustering large amounts of data. This algorithm clusters the data by observing similarity. It is an iterative process operating on a fixed number of k clusters (codebook vectors) that attempts to minimize some distance metric between the input vectors (unquantized data) and codebook vectors. Fig. 5(c) shows the distribution of clusters relative to the hologram data, compared to uniform quantization Fig. 5(b). One advantage of k-means nonuniform quantization over uniform is that no codebook vectors are wasted on unpopulated regions. This is quite visible in Fig. 5(b) where only 29 of the 49 uniform clusters are actually used.

Our subsequent experiments involved the use of unsupervised ANN techniques (Kohonen competitive and SOM) to quantize hologram data, with k-means used to compare performance. The ANNs were given an initial number of centers before training. Training was then performed for a fixed number of epochs, during which time each network used as many centers as it needed to cluster the input data. Generally, only a subset of the centers would be used, in contrast to k-means where all of the centers are utilized. For the initial codebook all initial cluster centroid positions are set to the midpoint of the input data and these continue to spread out over the input data as training proceeds. The distance that the codebook vector is moved depends on the learning rate. As explained in Section V, the Kohonen competitive network has both a learning rate and a conscience learning rate, while the SOM has an ordering learning rate and a tuning learning rate.

We performed extensive tests in order to determine the most appropriate ANN parameters for our data. The first set of experiments sought to determine how many training epochs would be required. A 32 × 32 pixel window of the die hologram was used. For training durations from 2 epochs through 2000 epochs, and for numbers of clusters from 9 through 81, the networks were trained with the hologram window. The trained networks were then used to quantize the full 1024 × 1024 pixel hologram and the resulting reconstructions U' by numerical propagation were compared with reconstructions U_0 from original (unquantized)

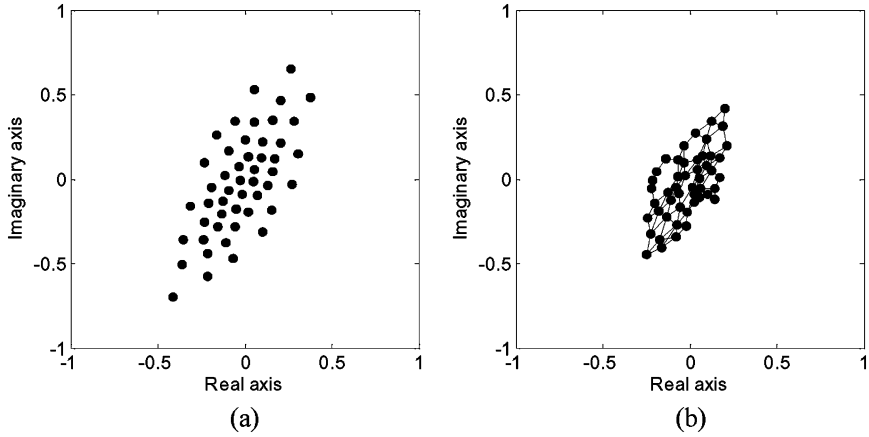

Fig. 7. Scatter plots of die complex-valued data, quantized with (a) Kohonen competitive and (b) SOM, both with 49 clusters.

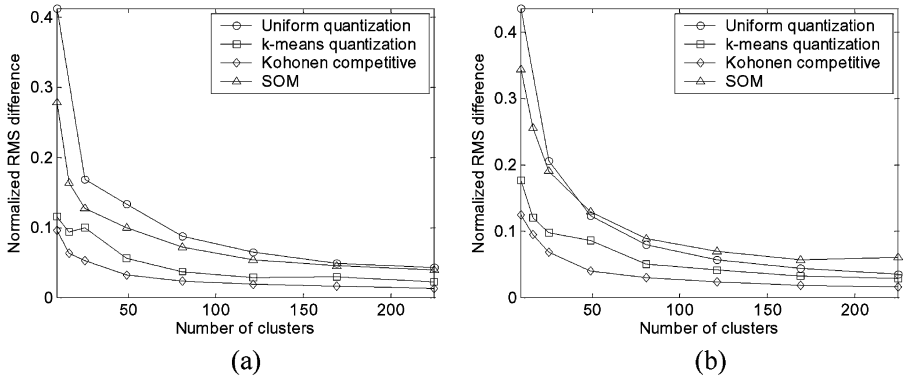

Fig. 8. NRMS difference in the reconstructed objects plotted against number of clusters: (a) die and (b) bolt.

versions of the holograms in terms of normalized rms (NRMS) difference between their intensities, defined as

$$D = \left[\sum_{m=0}^{N_x-1} \sum_{n=0}^{N_y-1} \left\{ |U_0(m,n)|^2 - |U'(m,n)|^2 \right\}^2 \times \left(\sum_{m=0}^{N_x-1} \sum_{n=0}^{N_y-1} \left\{ |U_0(m,n)|^2 \right\}^2 \right)^{-1} \right]^{1/2} \quad (5)$$

where (m,n) are discrete spatial coordinates in the reconstruction plane, and N_y and N_x are the height and width of the reconstructions, respectively. In order to lessen the effects of speckle noise, we examine only intensity in the reconstruction plane and apply a 5×5 pixel mean filtering operation prior to calculation of NRMS difference. The results for the Kohonen competitive network can be seen in Fig. 6(a). Since, for both types of network, in the order of 10^3 epochs produced only marginally better performance than 10^2 epochs, we chose 200 epochs as our default training duration.

Experiments were performed to determine an appropriate value for the conscience parameter of the Kohonen competitive network. It was found that all nonzero conscience learning rates were unsuitable for our white-noise-like digital hologram data. In these experiments, the number of neurons was set to be equal to the required number of clusters.

Appropriate learning rates had to be chosen for the ANNs. For these experiments, 128×128 pixel windows from each of the two holograms were used. For several learning rates, and for several numbers of clusters, the networks were trained on the hologram windows. After each training cycle of 200 epochs, the hologram was quantized using the network and the error in the hologram reconstruction measured. The results for the Kohonen competitive network and the die hologram are shown in Fig. 6(b). For the Kohonen competitive network, the learning rate of 0.1 was deemed the most appropriate. For the SOM, the combination of an ordering phase learning rate of 0.9 and a tuning phase learning rate of 0.1 was favored. For the SOM, the following additional parameter settings were chosen. A topology was chosen that creates a set of neurons that form a hexagonal pattern. We used $(\sqrt{n} \times \sqrt{n})$ as the dimensions of the i^{th} layer, where n was the number of clusters. We employed 1000 ordering phase steps, and set a tuning phase neighborhood distance equal to 1.

Having determined the appropriate parameters to get the best possible performance out of the two neural networks for our particular holographic data, we applied both networks to the compression of larger, 256×256 pixel, windows of both digital holograms. Fig. 7 shows the distribution of clusters for both the Kohonen competitive network and the SOM, for the die hologram and with 49 clusters. The Kohonen competitive network seems to allocate its clusters for greater coverage of the hologram data [recall Fig. 5(a)] than the SOM.

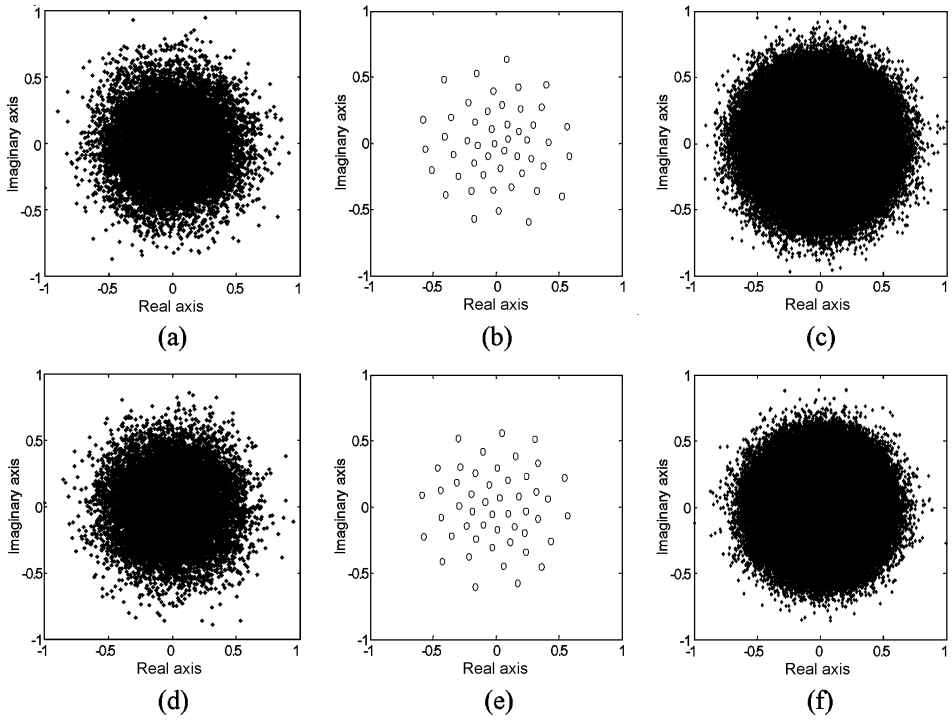

Fig. 9. Scatter plots of encrypted die data: 128 × 128 window (a) before quantization, (b) Kohonen competitive quantization, (c) 1024 × 1024 window before quantization; and in bolt: 128 × 128 window (d) before quantization, (e) Kohonen competitive quantization, (f) 1024 × 1024 window before quantization. (Color version available online at http://ieeexplore.ieee.org.)

The resulting NRMS reconstruction errors [calculated using (5)] for various numbers of clusters are compared in Fig. 8. Fewer numbers of clusters corresponds to a higher compression ratio. For comparison purposes, Fig. 8 also includes the NRMS error for uniform quantization and nonuniform k-means quantization. For both holograms, k-means clearly performs better than the SOM, which itself is only slightly better than uniform quantization. The Kohonen competitive network consistently beat the other techniques over all trials. Having identified the Kohonen competitive network as being the more appropriate unsupervised ANN for digital hologram compression, we next apply it to larger encrypted digital holograms.

VII. Quantization of Encrypted Digital Holograms

A uniform quantization technique was used to investigate the loss in reconstruction quality due to quantization in encrypted holograms, and to comparatively evaluate the quality of the results obtained using the Kohonen competitive neural network. The uniform quantization technique linearly rescaled the encrypted holograms to the square in the complex plane $[-1-i, 1+i]$ without changing their aspect ratio in the complex plane. The real and imaginary components of each holographic pixel were then quantized. The combined rescale and quantization operation is defined for individual pixels as

$$H'(x,y) = \text{round}\left[H(x,y) \times \sigma^{-1} \times \beta\right] \times \beta^{-1} \qquad (6)$$

and was applied to each pixel (x,y) in the encrypted hologram H, where

$$\sigma = \max\{|\min[\text{Im}(H)]|, |\max[\text{Im}(H)]|, |\min[\text{Re}(H)]|, |\max[\text{Re}(H)]|\} \qquad (7)$$

and where $\beta = 2^{(b-1)} - 1$. Here, b represents the number of bits per real and imaginary value, $\max(\cdot)$ returns the maximum scalar in its argument(s), and $\text{round}(\alpha)$ is defined as $\lfloor \alpha + 0.5 \rfloor$. After quantization, each real and imaginary value will be in the range $[-1, 1]$.

Nonuniform quantization was then employed to quantize the encrypted hologram data. The Kohonen competitive neural network was trained on a 128 × 128 pixel window of encrypted digital hologram data. We used the resulting centers to quantize the full 1024 × 1024 pixel encrypted digital hologram. Fig. 9(a) shows a scatter plot of the unquantized 128 × 128 pixel window of the die hologram that was used to train the ANN. Fig. 9(b) shows the cluster positions found by the ANN (equivalently, this is a scatter plot of the quantized encrypted data). Fig. 9(c) shows a scatter plot of the full 1024 × 1024 pixel hologram that the clusters from Fig. 9(b) were applied to. Figs. 9(d)–(f) show equivalent scatter plots for the bolt hologram.

Fig. 10 shows plots of NRMS difference against number of bits of encrypted holographic data for both uniform quantization and Kohonen competitive quantization. Fig. 10 illustrates the consistently lower NRMS error achieved by Kohonen competitive quantization over uniform quantization on our encrypted digital holograms. Further evidence of this performance gain achieved with nonuniform quantization is shown in Fig. 11 where we see the improved quality in the reconstructed objects using nonuniform quantization compared with uniform quantization. Reductions from 8 bytes to 4 bits, 3 bits, and 2 bits correspond to compression ratios of 16, 21, and 32, respectively.

Ideally, the cluster centers from one hologram could be stored in a lookup table and applied with reasonable results to the quantization of subsequent holograms. (The JPEG algorithm uses a

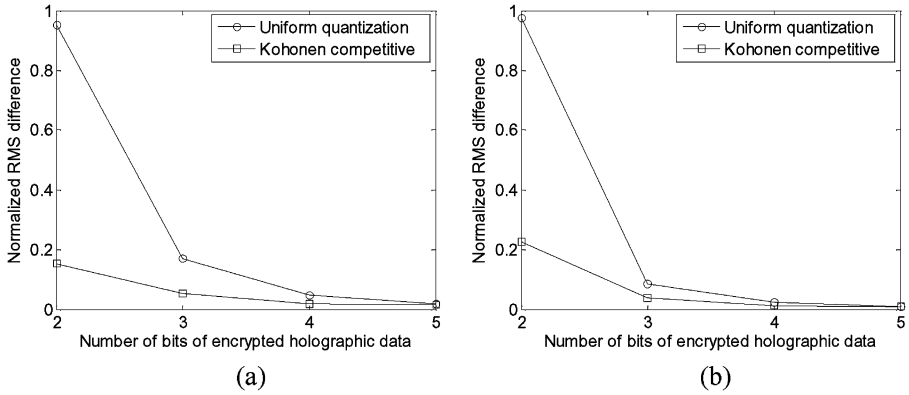

Fig. 10. NRMS intensity difference in decrypted and reconstructed 3D object images plotted against quantization level: (a) die and (b) bolt.

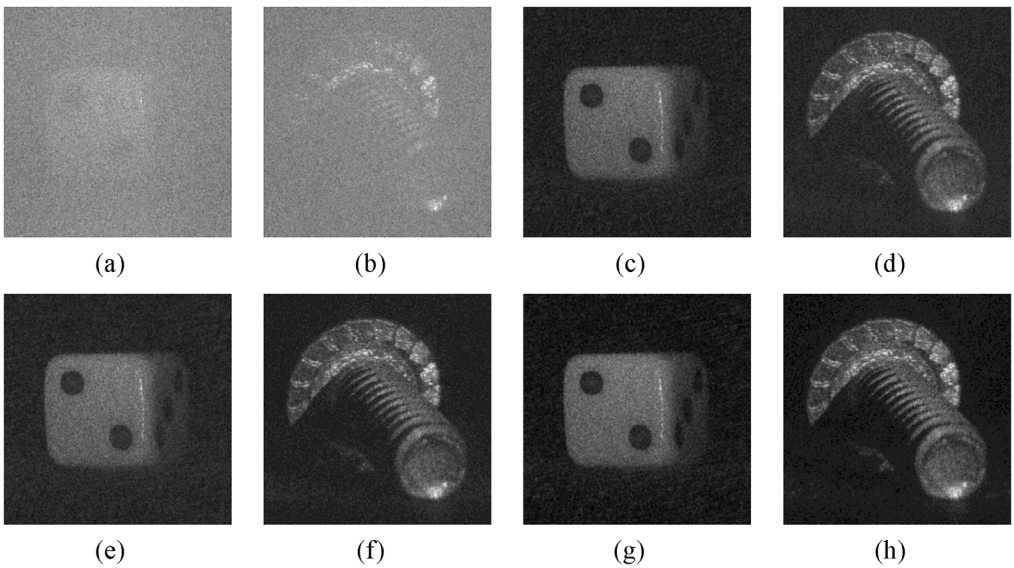

Fig. 11. Reconstructions from encrypted digital hologram data with uniform quantization (upper row) and Kohonen competitive quantization (lower row): (a), (b), (e), (f) 2 bits per real and imaginary value, and (c), (d), (g), (h) 3 bits per real and imaginary value. Mean filtering (5×5 pixel) applied in each case.

hard-coded lookup table of cosine-domain quantization values arrived at through performance evaluation over a database of sample input images.) We have found that the set of cluster centers we obtained from the Kohonen competitive neural network is very effective when applied in the quantization of a different hologram. This is illustrated in Fig. 12, where it can be seen that quantizing the die hologram using the centers obtained by applying Kohonen to the bolt hologram results in comparably low NRMS errors compared to those obtained when applying the centers produced specifically for the die hologram. By using the centers obtained from the Kohonen competitive network to quantize other encrypted holograms, we have the improved performance of nonuniform quantization combined with the speed advantage of uniform quantization.

VIII. Conclusion

This paper outlines an optical encryption technique, based on phase-shift digital holography, that is suitable for secure 3D object storage and transmission applications. This technique takes advantage of both the massive parallelism inherent in optical systems and the flexibility offered by digital electronics/software. Both the amplitude and phase of the hologram is encrypted by a phase-only perturbation of the Fresnel diffraction from the 3D object. Therefore, a phase mask is only required for this encryption scheme. Decryption and reconstruction of particular views of the 3D object can be performed optically or electronically. If the incorrect phase mask result is used, the reconstruction will be an unintelligible wavefront. Following encryption the hologram data is in a form suitable for digital electronic storage, transmission, or manipulation.

Lossless and lossy compression techniques were applied to the digital hologram data. Lossless techniques, such as LZ77, LZW, Huffman, and BW, perform very poorly on digital hologram data due to its white noise characteristics. We find that the encrypted digital holograms are compressed even less effectively. We evaluated two ANN-based nonuniform quantization techniques and found that the Kohonen competitive neural network performed best with our digital hologram data. We achieved reduced NRMS error and increased compression ratios using this technique. The Kohonen network was also shown to outperform the popular k-means clustering algorithm. We found that as few as 2 bits in each real and imaginary value

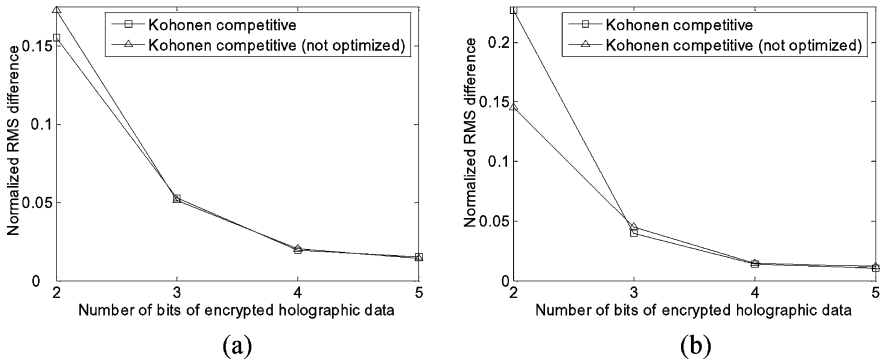

Fig. 12. NRMS intensity difference in the decrypted and reconstructed 3D objects plotted against quantization level, with uniform quantization and Kohonen competitive quantization: for (a) die and (b) bolt, where nonoptimized means using the Kohonen centers from the other hologram.

(corresponding to a compression ratio of 32) results in good quality decompressed and decrypted 3D object reconstructions. We have characterized the increase in quality as the number of bits is increased. This curve represents the upper bound on the resolution required of display devices in an optical decryption apparatus. If the nonuniform distributions of the pixel values can be determined then there may be more efficient ways to apply nonuniform quantization [32], [34]. Nonuniform quantization not only performs significant compression itself, it will also reduce the number of symbols (for Huffman) and introduce structure into the bit stream (for LZ77 and LZW) to allow them to perform further compression.

ACKNOWLEDGMENT

The authors wish to thank E. Tajahuerce and Y. Frauel for use of their hologram data.

REFERENCES

[1] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, vol. 33, no. 6, pp. 1752–1756, 1994.

[2] P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.

[3] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," *Appl. Opt.*, vol. 37, no. 35, pp. 8181–8186, 1998.

[4] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.*, vol. 24, no. 11, pp. 762–764, 1999.

[5] P. C. Mogensen and J. Glückstad, "Phase-only optical encryption," *Opt. Lett.*, vol. 25, no. 8, pp. 566–568, 2000.

[6] B. Javidi and T. Nomura, "Securing information by use of digital holography," *Opt. Lett.*, vol. 25, no. 1, pp. 28–30, 2000.

[7] S. Lai and M. A. Neifeld, "Digital wavefront reconstruction and its application to image encryption," *Opt. Commun.*, vol. 178, pp. 283–289, 2000.

[8] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, "Optoelectronic information encryption with phase-shifting interferometry," *Appl. Opt.*, vol. 39, no. 14, pp. 2313–2320, 2000.

[9] O. Matoba and B. Javidi, "Optical retrieval of encrypted digital holograms for secure real-time display," *Opt. Lett.*, vol. 27, no. 5, pp. 321–323, 2002.

[10] B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.*, vol. 28, no. 4, pp. 269–271, 2003.

[11] N. K. Nishchal, J. Joseph, and K. Singh, "Fully phase encryption using fractional Fourier transform," *Opt. Eng.*, vol. 42, no. 6, pp. 1583–1588, 2003.

[12] E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," *Appl. Opt.*, vol. 39, no. 35, pp. 6595–6601, 2000.

[13] T. J. Naughton and B. Javidi, "Compression of encrypted three-dimensional objects using digital holography," *Opt. Eng.*, vol. 43, no. 10, pp. 2233–2238, 2004.

[14] T. J. Naughton and B. Javidi, "Encryption and decryption of three-dimensional objects using digital holography," , in preparation.

[15] J. W. Goodman and R. W. Lawrence, "Digital image formation from electronically detected holograms," *Appl. Phys. Lett.*, vol. 11, pp. 77–79, 1967.

[16] T.-C. Poon and A. Korpel, "Optical transfer function of an acousto-optic heterodyning image processor," *Opt. Lett.*, vol. 4, pp. 317–319, 1979.

[17] L. Onural and P. D. Scott, "Digital decoding of in-line holograms," *Opt. Eng.*, vol. 26, no. 11, pp. 1124–1132, 1987.

[18] U. Schnars and W. P. O. Jüptner, "Direct recording of holograms by a CCD target and numerical reconstruction," *Appl. Opt.*, vol. 33, no. 2, pp. 179–181, 1994.

[19] J. H. Bruning, D. R. Herriott, J. E. Gallagher, D. P. Rosenfeld, A. D. White, and D. J. Brangaccio, "Digital wavefront measuring interferometer for testing optical surfaces and lenses," *Appl. Opt.*, vol. 13, no. 11, pp. 2693–2703, 1974.

[20] J. Schwider, B. Burow, K. E. Elsner, J. Grzanna, R. Spolaczyk, and K. Merkel, "Digital wavefront measuring interferometry: some systematic error sources," *Appl. Opt.*, vol. 22, no. 21, pp. 3421–3432, 1983.

[21] I. Yamaguchi and T. Zhang, "Phase-shifting digital holography," *Opt. Lett.*, vol. 22, no. 16, pp. 1268–1270, 1997.

[22] B. Javidi and E. Tajahuerce, "Three-dimensional object recognition by use of digital holography," *Opt. Lett.*, vol. 25, no. 9, pp. 610–612, 2000.

[23] Y. Frauel, E. Tajahuerce, M.-A. Castro, and B. Javidi, "Distortion-tolerant three-dimensional object recognition with digital holography," *Appl. Opt.*, vol. 40, no. 23, pp. 3887–3893, 2001.

[24] T. J. Naughton, Y. Frauel, B. Javidi, and E. Tajahuerce, "Compression of digital holograms for three-dimensional object reconstruction and recognition," *Appl. Opt.*, vol. 41, no. 20, pp. 4124–4132, 2002.

[25] O. Matoba, T. J. Naughton, Y. Frauel, N. Bertaux, and B. Javidi, "Real-time three-dimensional object reconstruction by use of a phase-encoded digital hologram," *Appl. Opt.*, vol. 41, no. 29, pp. 6187–6192, 2002.

[26] J. W. Goodman and A. M. Silvestri, "Some effects of Fourier-domain phase quantization," *IBM J. Res. Develop.*, vol. 14, pp. 478–484, 1970.

[27] W. J. Dallas and A. W. Lohmann, "Phase quantization in holograms—depth effects," *Appl. Opt.*, vol. 11, no. 1, pp. 192–194, 1972.

[28] T. Nomura, A. Okazaki, M. Kameda, Y. Morimoto, and B. Javidi, "Image reconstruction from compressed encrypted digital hologram," *Opt. Eng.*, vol. 44, no. 7, pp. 075801-1–075801-7, 2005.

[29] T. J. Naughton, J. B. Mc. Donald, and B. Javidi, "Efficient compression of Fresnel fields for internet transmission of three-dimensional images," *Appl. Opt.*, vol. 42, no. 23, pp. 4758–4764, 2003.

[30] D. Kayser, T. Kreis, and W. Jüptner, "Compression of digital holographic data using its electromagnetic field properties," in *Proc. SPIE*, 2005, vol. 5908, pp. 97–105.

[31] A. E. Shortt, T. J. Naughton, and B. Javidi, "Compression of digital holograms of three-dimensional objects using wavelets," *Opt. Express*, vol. 14, no. 7, pp. 2625–2630, 2006.

[32] ——, "A companding approach for nonuniform quantization of digital holograms of three-dimensional objects," *Opt. Express*, vol. 14, no. 12, pp. 5129–5134, 2006.
[33] ——, "Quantization compression of digital holograms of three-dimensional objects using artificial neural networks," submitted for publication..
[34] ——, "Histogram approaches for lossy compression of digital holograms of three-dimensional objects," , submitted for publication.
[35] ——, "Nonuniform quantization compression of digital holograms," *Opt. Lett.*, 2006, submitted for publication.
[36] I. Yamaguchi, K. Yamamoto, G. A. Mills, and M. Yokota, "Image reconstruction only by phase in phase-shifting digital holography," *Appl. Opt.*, vol. 45, no. 5, pp. 975–983, Feb. 2006.
[37] E. Darakis and J. J. Soraghan, "Compression of interference patterns with application to phase-shifting digital holography," *Appl. Opt.*, vol. 45, no. 11, pp. 2437–2443, 2006.
[38] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," *Opt. Eng.*, vol. 36, no. 4, pp. 992–998, 1997.
[39] F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, "Influence of a perturbation in a double phase-encoding system," *J. Opt. Soc. Am. A*, vol. 15, no. 10, pp. 2629–2638, 1998.
[40] J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. New York: McGraw-Hill, 1996.
[41] H. J. Caulfield, *Handbook of Optical Holography*. New York: Academic, 1979.
[42] D. A. Huffman, "A method for the construction of minimum redundancy codes," *Proc. IRE*, vol. 40, pp. 1098–1101, Sep. 1952.
[43] J. Ziv and A. Lempel, "A universal algorithm for sequential data compression," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 3, pp. 337–343, May 1977.
[44] T. A. Welch, "A technique for high performance data compression," *IEEE Computer*, vol. 17, no. 6, pp. 8–19, 1984.
[45] M. Burrows and D. J. Wheeler, A block-sorting lossless data compression algorithm Digital Systems Research Center, Palo Alto, CA, Tech. Rep. 124, 1994.
[46] N. M. Nasrabadi and Y. Feng, "Vector quantization of images based upon the Kohonen self-organizing feature maps," in *IEEE Int. Conf. Neural Netw.*, 1988, vol. 1, pp. 101–108.
[47] C. Amerijckx, M. Verleysen, P. Thissen, and J.-D. Legat, "Image compression by self-organized Kohonen map," *IEEE Trans. Neural Netw.*, vol. 9, no. 3, pp. 503–507, 1998.
[48] P. V. Balakrishnan, M. C. Cooper, V. S. Jacob, and P. A. Lewis, "A study of the classification capabilities of neural networks using unsupervised learning: a comparison with k-means clustering," *Psychometrika*, vol. 59, no. 4, pp. 509–525, 1994.
[49] R. D. Dony and S. Haykin, "Neural network approaches to image compression," *Proc. IEEE*, vol. 83, no. 2, pp. 288–303, Feb. 1995.
[50] M. Egmont-Peterson, D. de Riddler, and H. Handels, "Image processing with neural networks—a review," *Pattern Recogn.*, vol. 35, pp. 2279–2301, 2002.
[51] J. Jiang, "Image compression with neural networks—a survey," *Signal Process. Image Commun.*, vol. 14, pp. 737–760, 1999.
[52] A. K. Krishnamurthy, S. C. Ahalt, D. E. Melton, and P. Chen, "Neural networks for vector quantization of speech and images," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 8, pp. 1449–1457, Oct. 1990.
[53] C.-C. Lu and Y. H. Shin, "A neural network based image compression system," *IEEE Trans. Consum. Electron.*, vol. 38, no. 1, pp. 25–29, Feb. 1992.
[54] T. Kohonen, *Self-Organizing Maps*. Berlin, Germany: Springer-Verlag, 1994.
[55] ——, "The self-organizing map," *Proc. IEEE*, vol. 78, no. 9, pp. 1464–1480, Sep. 1990.
[56] J. MacQueen, "Some methods for classification and analysis of multivariate observations," in *Proc. 5th Berkeley Symp. on Math. Statistics and Probab.*, 1967, vol. 1, pp. 281–297.

Alison E. Shortt received the B.Sc. degree (single honors) in computer science from the National University of Ireland, Maynooth (formerly St. Patrick's College), Maynooth, Ireland, in 1999, and the Ph.D. degree in 2006.

She is currently a postdoctoral researcher at the Department of Electrical and Computer Engineering, University of Connecticut, Storrs. Her research interests include digital holography and compression.

Thomas J. Naughton received the B.Sc. degree (double honors) in computer science and experimental physics from the National University of Ireland, Maynooth (formerly St. Patrick's College), Maynooth, Ireland, in 1995.

He has worked at Space Technology (Ireland) Ltd. and has been a visiting researcher at the Department of Radioelectronics, Czech Technical University, Prague, Czech Republic, and the Department of Electrical and Computer Engineering, University of Connecticut, Storrs. He is currently a Lecturer in the Department of Computer Science, National University of Ireland, Maynooth. In this department, he leads research groups in optical information processing, computer theory (optical and biological models of computation), distributed computing, and bioinformatics. He has published over 20 international journal articles and book chapters in these areas.

Mr. Naughton is a member of IEEE LEOS, the Association for Computing Machinery (ACM), the Optical Society of America (OSA), and SPIE.

Bahram Javidi (S'82–M'83–SM'96–F'98) received the B.S. degree in electrical engineering from George Washington University, Washington, DC, and the M.S. degree and Ph.D. degrees in electrical engineering from the Pennsylvania State University, Philadelphia.

He is the Board of Trustees Distingushed Professor with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs. He has completed several books including *Optical and Digital Techniques for Information Security* (Springer, 2003), *Image Recognition: Algorithms, Systems, and Applications* (Marcel Dekker, 2002), *Three Dimensional Television, Video, and Display Technologies* (Springer Verlag, 2002), Smart Imaging Systems (SPIE Press, 2001), *Real-time Optical Information Processing* (Academic Press, 1994), and *Optical Pattern Recognition* (SPIE Press, 1994). He has published over 170 technical papers in major journals, including *Physics Today and Nature*, and his research has been cited in *IEEE Spectrum*, *Science*, and *New Scientist*.

Dr. Javidi is a Board of Trustees Distinguished Professor of Electrical and Computer Engineering with the University of Connecticut. Dr. Javidi is a fellow of the IEEE, the OSA, and the SPIE. He received the IEEE Lasers and Electro-optics Society Distinguished Lecturer Award in 2003, the IEEE Best Journal Paper Award from IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2002, the University of Connecticut Alumni Association Excellence in Research Award, the Chancellor's Research Excellence Award, and the first Electrical and Computer Engineering Department Outstanding Research Award.