Image encryption based on phase encoding by means of a fringe pattern and computational algorithms

J.A. Muñoz Rodríguez and R. Rodríguez-Vera
Centro de Investigaciones en Optica A.C.,
Apartado Postal 1- 948, León, GTO, 37000, México
e-mail: munoza@foton.cio.mx

Recibido el 23 de agosto de 2006; aceptado el 26 de enero de 2006

A computational technique for image encryption and decryption is presented. The technique is based on light reflection, intensity superposition and computational algorithms. The image to be encrypted is a reflectance map obtained by means of the light reflected by a scene. To perform the encryption procedure, the image is encoded in a computer-generated fringe pattern. The model of the fringe pattern is a cosine function, which adds to its argument the image to be encrypted as a phase. It generates a fringe pattern deformed according to the image. To complete the encryption, a random mask is superimposed on the fringe pattern. The decryption procedure is performed by subtracting the random mask from the encrypted image and applying a phase recovery method. To retrieve the phase from the fringe pattern, the heterodyne demodulation method is used. To describe the accuracy of results of the decrypted images and the robustness of the encryption, a root mean square of error is calculated. All steps of the encryption and decryption are performed in computational form. The results of encryption and decryption are thus improved. It represents a contribution to the field of encryption and decryption. This technique is tested with simulated images and real images, and its results are presented.

Keywords: Reflectance map; encryption and decryption; fringe pattern; phase recovery method.

Se presenta una técnica computacional para encriptación y desencriptación de imágenes. Esta técnica esta basada en la reflexión de la luz, superposición de intensidad y algoritmos computacionales. La imagen a ser encriptada es un mapa de reflectancia obtenida por medio de la luz reflejada por una escena. Para efectuar el procedimiento de encriptación, la imagen es codificada en un patrón de franjas generado por computadora. El modelo del patrón de franjas es una función coseno, la cual agrega en su argumento la imagen a ser encriptada como una fase. Esto genera un patrón de franjas deformado de acuerdo a la imagen. Para completar la encriptación, se sobrepone una máscara aleatoria sobre el patrón de franjas. El procedimiento de desencriptación es efectuado substrayendo la máscara aleatoria de la imagen encriptada y aplicando un método de recuperación de fase. Para extraer la fase del patrón de franjas, se usa el método de demodulación heterodino. Para describir la precisión de los resultados de imágenes desencriptadas y la robustés de la encriptación, se calcula la raíz del error cuadrático medio. Todos los pasos de la encriptación y desencriptación se efectúan en forma computacional. De esta manera, los resultados de encriptación y desencriptación son mejorados. Esto representa una contribución en el campo de la encriptación y desencriptación. Esta técnica es probada con imágenes simuladas y con imágenes reales, y sus resultados son presentados.

Descriptores: Mapa de reflectancia; encriptación y desencriptación; patrón de franjas; método de recuperación de fase.

PACS: 42.30.R; 07.05.P; 42.30.W; 02.70

1. Introduction

With the fast progression of data exchange electronically, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Optics provides flexibility in encodeing information by using features of the light. Security systems have been developed by means of optical processing. Among them are random phase encoding [1-4], digital holography [5-8], Fractional Fourier transform [9-12], virtual (digital) optics [13-14], optical exclusive-OR [15-16], watermarking [17-19], and polarization [20-21]. These methods use a complete optical set-up which include lenses, source light, splitters, mirrors, spatial filters, gratings, etc. The main parameters of an encryption system are robustness of the encryption, the quality of the decrypted image, and the processing time. With the advances in computer performance and electronic devices for image acquisition, encryption and decryption can be produced using light features. It represents a valuable tool for improving the robustness of the encryption, the quality of the retrieved image, and the processing time. The architecture of the technique proposed in this paper is completely computational. The optic approach in this technique is light reflection, phase encoding and intensity superposition. The image to be encrypted is a reflectance map obtained by means of the light reflected by a scene. Intensity superposition is used to obtain the intensity pattern of the image encryption. The encryption procedure of this technique is based on a phase encoding. The phase is represented by the reflectance map of the image to be encrypted. Using a computational procedure, the image encryption is performed based on the procedure of an optical set-up. The encryption is carried out by means of a computer-generated fringe pattern. The model of this fringe pattern is a cosine function, which adds tp its argument the reflectance map of the image as a phase. The result of this procedure is a fringe pattern deformed according to the image intensity. To complete the encryption a random mask is superimposed on the fringe deformations. The decryption procedure for retrieving the original image is performed subtracting the key random mask from the encrypted image and detecting the phase from the fringe pattern. The phase recovery method applied in this technique is the heterodyne demodulation method (**HDM**), which is also called the direct interferometry method [22]. The set-up for encryption and decryption includes a CCD camera, frame grabber and computer. The camera captures the intensity reflected by a scene. The intensity recorded in matrix form by the camera is the reflectance map, which represents the phase for the encryption. By means the frame grabber, the reflectance map is converted to a digital image, whose values are in grey-levels. The computer performs the algorithms for encryption and decryption based on light features. To elucidate the contribution of this technique, the results obtained are evaluated based on the root mean square (*rms*) of error and signal-to-noise ratio (SNR). This analysis includes the robustness of the encryption and the quality of the retrieved image. Finally, the processing time for carrying out encryption and decryption is presented.

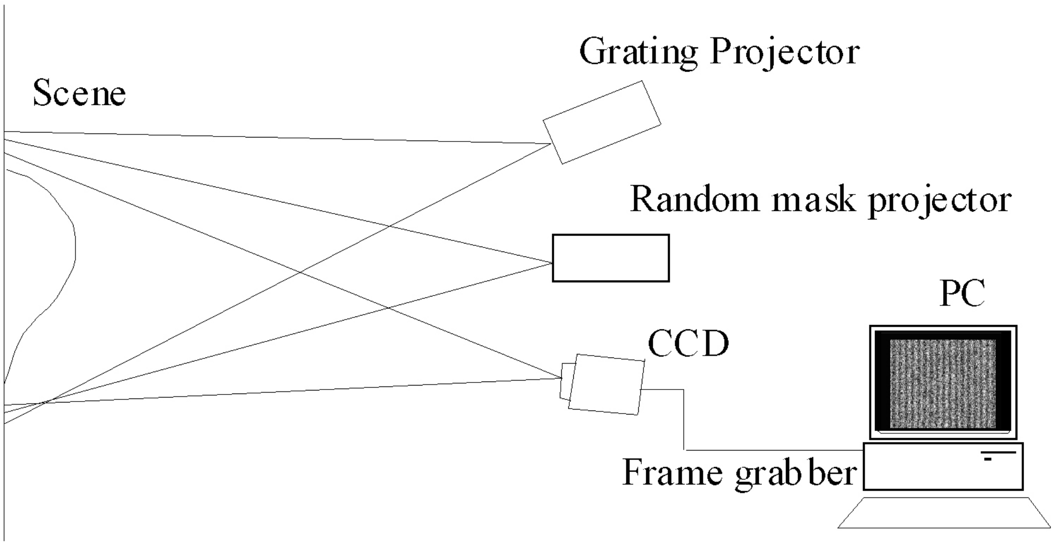

FIGURE 1. Set-up of the light projection technique.

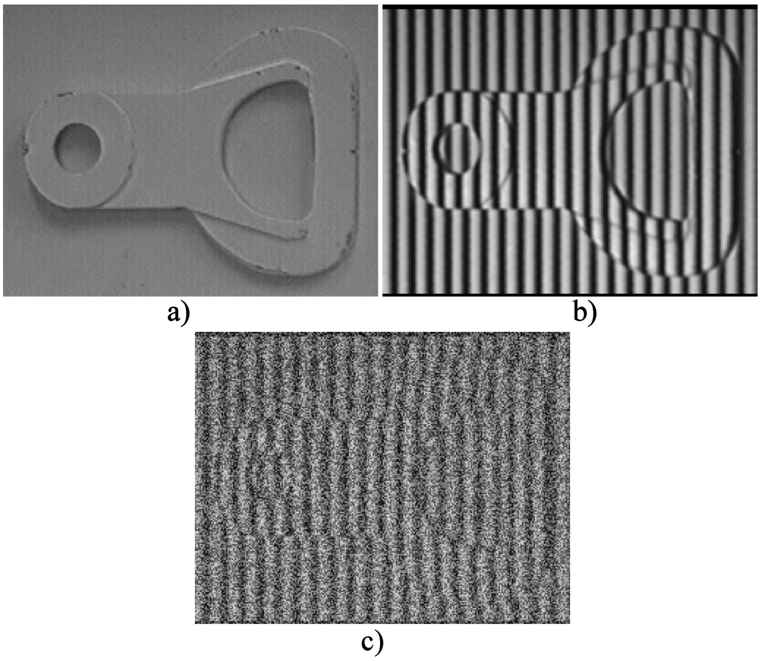

FIGURE 2. (a) Scene to be encrypted; (b) Image of the grating projected on the scene; and (c) Encryption of the scene in superimposing the random mask on the projected grating.

2. Basic theory

Visual cryptography is a powerful method for sharing and encrypting information, especially images [23-24]. The simplest version of visual cryptography assumes that the original image is handled like other pixel collections, which generate a secret image. The image to be encrypted is represented by grey-level pixels in matrix form. The intensity values of the pixels in a digital image are the result of recording the light reflected by a scene [25]. The amount of light radiated from a scene is called radiance [26]. A standardized representation of the light radiated from a scene is a reflectance map [27]. This reflectance map is converted to grey-levels by means of a frame grabber. In this procedure, an electrical signal proportional to the light intensity is produced. In optics and computer vision, a grey-level image and the reflectance map are equivalent. Therefore, the reflectance map can be represented in matrix form as an image by

$$\phi(i,j) = I \tag{1}$$

where $\phi(i,j)$ is the image represented by a matrix of pixels, I is the pixel intensity represented by the grey-level, and (i,j) are the coordinates of the pixel position. The coordinates i, j are only integers. In this manner, a grey-level image to be encrypted is defined. To perform the image encryption, features of the light projection are applied in computational form. In the encryption, firstly, the image is encoded by means of a fringe pattern. Secondly, to complete the encryption, a random mask is superimposed on the fringe pattern. The basic concept of using these two steps for the encryption is based on the procedure of an optical set-up. Therefore, the encryption is performed using a computational procedure similar to the procedure of an optical set-up. The optical arrangement in which the encryption is based corresponds to light projection. Fig. 1 shows the set-up of the light projection technique. This set-up consists of a random mask projector, a grating projector, a CCD camera, and a computer. Fig. 2a shows a scene to be encrypted by means of light projection technique. To do this, the grating is projected onto the scene. The intensity profile projected by the grating is a cosine function which is described by

$$g(x,y) = a + b\cos[2\pi f_0 x], \tag{2}$$

where a and b are the background intensity and contrast of the light projected by the grating, and f_0 is the fundamental frequency [28]. When a grating is projected onto a scene, the fringes suffer deformations in the image plane. This is due to the scene topography when the viewer is looking from a different direction from the grating projection. The fringe deformation is represented as a phase $\phi(x,y)$. The intensity profile of the fringes deformed is described by the following equation:

$$gd(x,y) = a + b\cos[2\pi f_0 x + \phi(x,y)]. \tag{3}$$

From this intensity pattern, fringe deformations are observed. To hide the fringe deformations, a random mask is superimposed on the intensity pattern. The intensity profile projected by a random mask is defined as $\mathrm{Rand}(x,y)$. The superimposing of two intensity patterns can be determined by the addition of these two intensity patterns [28]. Therefore, the intensity observed of these two patterns projected onto the scene is determined by

$$I_E(x,y) = \mathrm{Rand}(x,y) + gd(x,y), \tag{4}$$

where $I_E(x,y)$ is the result of the encryption, $\mathrm{Rand}(x,y)$ is random mask, and $gd(x,y)$ is the deformed fringe pattern given by Eq. (3). The observed intensity of the patterns given by Eq. (2), Eq. (3) and Eq. (4) are represented in the continuous space. It is indicated by the coordinates (x,y), which represent the intensity position in continuous space. To show the steps of the encryption given by Eq. (3) and Eq. (4), two images are captured. The images captured from these intensity patterns are represented by a pixel matrix in grey level. Fig. 2b shows the fringe pattern that was captured from the grating projected onto the scene. This image corresponds to a fringe pattern deformed according to the scene of Fig. 2a. The intensity pattern captured from the random mask superimposed onto the fringe pattern is shown in Fig. 2c. This image corresponds to the encryption of the scene in Fig. 2a. This encryption performed by means of the light projection technique can be reproduced in computational form. This procedure can be obtained by creating a random mask and a grating by means of computer algorithms. Also, the operation of superimposing two intensity patterns can be performed by means of a computational procedure. The encryption procedure using computational algorithms is described in Sec. 3.

3. Image encryption and decryption

Image encryption assumes that the original image $\phi(i,j)$ is handled like any other pixel collection to create a secret image. In this technique, the visual secret is obtained using a computational procedure based on the encryption performed by the light projection technique. In the same manner, the encryption in computational form is performed by means of a fringe pattern and a random mask. The original image is encoded in the fringe pattern. Then, the random mask is superimposed over the fringe pattern to complete the encryption. The same scene encrypted by the light projection set-up is used to make the encryption by computer algorithms. To carry it out, this scene is captured by the CCD camera. The intensity captured by the CCD camera corresponds to the reflectance map of the scene [27]. Using a frame grabber this reflectance map of the scene is converted to a digital image $\phi(i,j)$. This scene corresponds to the image shown in Fig. 2a. In this case, the intensity of the image $\phi(i,j)$ is represented as a phase. To perform the encryption, the image is encoded in a fringe pattern. To do this, a fringe pattern is generated in computational form as a cosine function. In this fringe pattern, the intensity of the image $\phi(i,j)$ is added into the

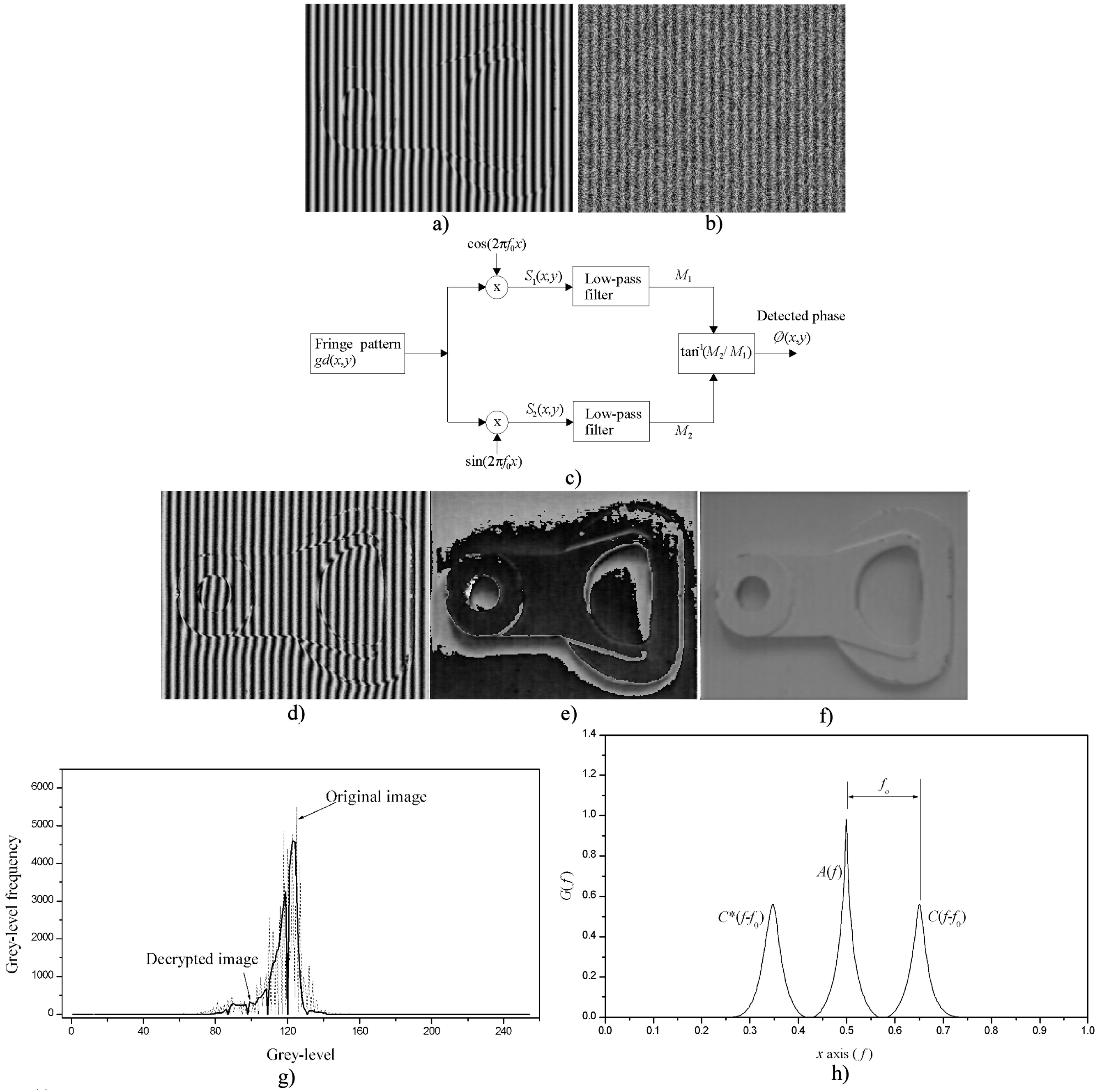

FIGURE 3. (a) Deformed fringe pattern according to the scene in Fig. 2a; (b) Image encryption of the image of Fig. 2a by means of Eq. (6); (c) Typical heterodyne demodulation scheme; (d) Fringe pattern with phase values greater than 2π; (e) Wrapped phase calculated by Eq. (12) from the fringe pattern Fig. 3d; (f) Phase retrieved from fringe pattern of Fig. 3a by using Eq. (12); (g) Histogram of the decrypted image and the histogram of the original image; and (h) Spatial frequency f_o deduced by separating the carrier frequency.

argument of the cosine function as a phase. This relation is represented by the following equation:

$$Fp(i,j) = a + b\cos[2\pi f_0 i + \phi(i,j)], \qquad (5)$$

Eq. (5) represents a fringe pattern deformed according to the image $\phi(i,j)$. By substituting the image $\phi(i,j)$ of Fig. 2a into Eq.(5), a deformed fringe pattern is generated. The image of this fringe pattern is shown in Fig. 3a. To hide the fringe deformations, a random mask is superimposed on the fringe pattern. The random mask in computational form is defined by *rand*$(i,\ j)$. As in light projection technique, the superimposing is determined by the addition of two intensity patterns. Therefore, the final version of image encryption is determined by

$$Im_E(i,j) = rand(i,j) + Fp(i,j), \qquad (6)$$

where $Im_E(i,\ j)$ is the final result of the encrypted image. The image encryption of Fig. 2a by means of Eq.(6) is shown in Fig. 3b. With this step, the encryption procedure has been completed. The results obtained in computational form are similar to the results obtained by the optical set-up, as shown in Figs. 3a and 3b. Now, the fringe pattern and random mask are the code for retrieving the original image. This is because the phase of the fringe pattern contains the information of the original image. To perform the decryption procedure, the random mask is subtracted from the encrypted image. It is computed using the following relation:

$$Fd(i,j) = Im_E(i,j) - rand(i,j). \qquad (7)$$

The result of applying Eq.(7) is a fringe pattern corresponding to Fig. 3a. To retrieve the original image from the deformed fringe pattern, a phase detection method is applied. To carry it out, the phase is extracted from the fringe pattern by means of the **HDM** [29]. A typical heterodyne demodulation scheme is shown in Fig. 3c. The heterodyne method involves multiplying an unknown function by a sinusoidal reference and integrating to filter out the low frequency of the product. This algorithm is performed by the multiplication of the deformed fringe pattern by sine and cosine of the reference carried signal to obtain two image fields. These two images can be described by the following equations:

$$S_1(i,j) = Fd(i,j)\sin(2\pi f_0 i), \qquad (8)$$

$$S_2(i,j) = Fd(i,j)\cos(2\pi f_0 i). \qquad (9)$$

Then, a smoothing process over these two fields is performed to remove the interfering signal at twice the carrier frequency obtained as a consequence of the sine and cosine. This step is obtained by the following relations:

$$M_1(i,j) = h(i,j) * [Fd(i,j)\sin(2\pi f_0 i)], \qquad (10)$$

$$M_2(i,j) = h(i,j) * [Fd(i,j)\cos(2\pi f_0 i)], \qquad (11)$$

where the asterisk denotes convolution and $h(i,\, j)$ is a low-pass filter, which can be a single average window. By means of the arctan function, the phase is obtained by the expression

$$\phi(i,j) = \arctan\left[\frac{M_2(i,j)}{M_1(i,j)}\right]. \qquad (12)$$

The phase calculated by Eq. (12) is determined in the interval between -π and π. This is due to the arctan function, which gives values in the interval between -π and π. Therefore, when the fringe pattern contains phase values greater than 2π, the phase map calculated by Eq. (12) is wrapped. This means that the phase calculated contains discontinuities of 2π. Therefore, for removing these discontinuities, an unwrapping step is necessary to construct a continuous phase. Figure 3d shows a fringe pattern which contains phase values greater than 2π. Figure 3e shows the wrapped phase calculated by Eq. (12), which contains discontinuities of 2π. To avoid the unwrapping step, the fringe pattern should contain phase values in the range -$\pi < \phi(i,j) < \pi$. To obtain a fringe pattern with phase value in this range, the grey-levels of the original image $\phi(i,j)$ should be converted to this range. As the image represented by a phase has no negative values, the interval should be 0< $\phi(i,j) < \pi$. To obtain phase values in this range, the grey-level values of the original image are normalized into the range between 0 and 0.95π. Then the 256 grey-level values are less than 0.95π. Therefore, the phase encoded into the fringe pattern $Fd(i,j)$ contain only values ranging from 0 to 0.95π. Applying this criterion, the fringe pattern created by Eq. (5) does not contains phase values greater than π. In this manner, the phase obtained by Eq. (12) does not contain discontinuities greater than 2π, and the unwrapping step is unnecessary. Figure 3f shows the phase retrieved from fringe pattern of Fig. 3a by using Eq. (12). With this procedure, the original image has been retrieved as the phase $\phi(i,j)$. The result of decryption is a version of the original image that is slightly smooth. In this manner, the original image can be recovered by detecting the phase from the fringe pattern. To see the variation in the grey-level of the decrypted image with respect to the original image, its histograms are calculated. Figure 3g shows the histogram of the decrypted image and the histogram of the original image. In this figure, the histogram of the decrypted image is indicated by the solid line and the histogram of the original image is indicated by the dashed line. In Sec. 4, the difference between these two histograms is discussed. To determine spatial frequency f_o used by Eq. (8) and Eq. (9), Fourier transform is applied. For fringes generated parallel to y-axis, the carrier signal involves only x-component. In this case, the Fourier transform is described by

$$FT\,[g(x)] = G(f) = \int_{-\infty}^{\infty} \exp(-j2\pi f x) g(x) dx, \qquad (13)$$

$$G(f) = A(f) + C(f - f_0) + C * (f + f_0). \qquad (14)$$

The functions in Eq. (14) denote Fourier transforms of the corresponding quantities in the spatial domain, and f_0 is the spatial frequency in the x-direction. The result of this procedure is the frequency spectra shown in Fig. 2h. The spatial frequency f_o is deduced by separating the carrier frequency as shown in Fig. 2h.

4. Experimental results and discussions

The set-up used in this technique is completely computational. Based on a procedure similar to an optical set-up, this set-up performs image encryption by means of computer algorithms. As the set-up is completely computational, the optical components are avoided. Fig. 4 shows the computational set-up. In this set-up, the image to be encrypted is captured by the CCD camera and digitized by a frame grabber with a resolution of 256 × 256 pixels and 255 grey-levels. Fig. 5a, shows the image of the face of an actress to be encrypted. To do this, the pixels of the image are normalized into intervals between 0 and 0.95π. Then this image $\phi(i,j)$ is used as a phase to generate a deformed fringe pattern by means of Eq. (5). By substituting these normalized values of the image of Fig. 5a into Eq. (5), a deformed fringe pattern is obtained. The grey-level of the background intensity of the fringe pattern is defined as a =60 and the contrast b=60. In this manner, the variation of the grey-level of the fringe pattern is divided into intervals from 0 to 120. The fringe pattern deformed according to the original image is shown in Fig. 5b. The fringe deformations are hidden by means of a random mask using Eq. (6). The random mask *rand*$(i,\, j)$ is a computer-generated grey-level image. This image contains pixels whose grey-level values are divided into intervals from 0 to 135, randomly. The final result of the encrypted image *Im*$_E(i,\, j)$ is shown in Fig. 5c. In this manner, the encryption procedure has been completed. Now, to retrieve the original image, the random mask *rand*$(i,\, j)$ and the fringe pattern *Fd*(i,j) are the key code. To perform the decryption procedure by means of Eq.(7), the random mask is subtracted from the encrypted image, Fig. 5(c). The result of this step is the same fringe pattern shown in Fig.5(b). The intensity distribution of this fringe pattern contains the original image encoded as a phase. To extract the phase information from the image *Fd*(i,j), the **HDM** is applied. To do this, the spatial frequency f_o is determined by applying the Fourier transform in Eqs. (13) and (14) to the fringe pattern. The spatial frequency f_o is deduced by the separation of the carrier frequency. To avoid this process, the value of the frequencyf_o is included in the file of the encrypted image. This frequencyf_o is substituted into Eq. (8) and Eq. (9). Then, $M_1(i,\, j)$ and $M_2(i,\, j)$ are computed to obtain the phase by means of Eq. (12). The result of this step is a continuous phase division into intervals from 0 to 0.95π, as shown in Fig. 5d. As this image does not contain discontinuities of 2π unwrapping procedure is not necessary. This result is a version of the original image, as shown in Fig. 5a. The variation of the grey-level values of the decrypted image with respect to the original image is shown by means of histograms. Figure 5e shows the histograms of the decrypted and the original images. In this figure, the histogram of the decryption is indicated by the solid line and the histogram of the original image is indicated by the dashed line. In this manner, image decryption has been completed.

The parameters to achieve a good result in the encryption and decryption are frequency f_o and the reflectance map of the image. The choice of frequency f_o has a great influence in the behaviour of the fringe pattern. For the encryption, the frequency value should be a period greater than 3 pixels. When the frequencyf_o contains a period of less than 2 pixels, the fringe pattern is not determined on the screen and encryption is not achieved. The result of applying frequency of a period of 1.0 pixel into Eq. (5) is shown in Fig. 6a. In this image, a version of the original image can be observed. By means of Eq. (6), the random mask is superimposed on the image of Fig. 6a and the result is shown in Fig. 6b. This result also shows a version of the original image. With respect to the reflectance map of the image $\phi(i,j)$, it should be normalized to values of less than π radians to avoid the unwrapping step. Also, when the reflectance map of the image $\phi(i,j)$ contains values greater than 10π radians, the fringe pattern is destroyed. Figure 6c shows a fringe pattern with an image $\phi(i,j)$ whose values normalized to 14π radians. When the frequency f_o and the original image are above the values mentioned, the phase recovery method cannot be applied for the decryption process. This is because the encrypted image is not a fringe pattern. In this case, the decryption process cannot recover the original image. To find the accuracy of results of the images decrypted and robustness of the encryption, a root mean square (*rms*) of error is calculated [30]. These criteria provide the error between input image and output image. The *rms* value can be described by the following relation:

$$rms = \sqrt{\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}[g(i,j) - f(i,j)]^2}, \qquad (15)$$

where $g(i,j)$ is the pixel intensity of the original image, $f(i,j)$ is the pixel intensity of the decrypted image. The row

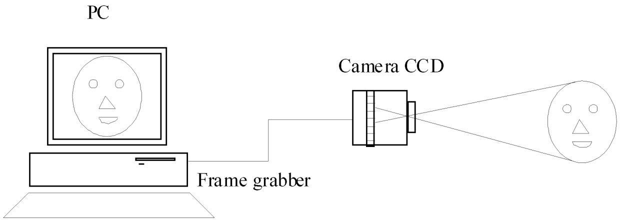

FIGURE 4. Comput set-up.

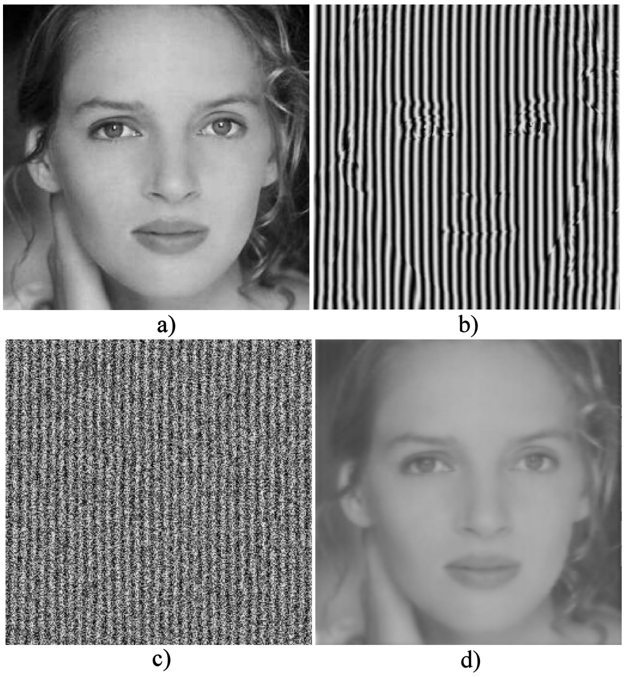

FIGURE 5. (a) Image of an actress; (b) Fringe pattern deformed according to the image of Fig. 5a; (c) Image of the actress encrypted by the fringe pattern and random mask; (d) Decrypted image of the actress using Eq. (12); and (e) Histograms of the decrypted image Fig. 5d and the original image Fig. 5a.

and column numbers of these two images are defined by N. To determine the quality of the decrypted image, the difference between the original image and the decrypted image is computed. To determine the difference between the original and decrypted images, the *rms* signal-to-noise ratio (*SNR*)$_{rms}$ is calculated [31]. The (*SNR*)$_{rms}$ is given by

$$(SNR)_{rms} = \sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{N} g^2(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} [g(i,j) - f(i,j)]^2}}, \tag{16}$$

where the variable term in the denominator is the noise expressed in terms of the original and the decrypted images. An alternative definition of signal-to-noise ratio is the square root of the peak value of the original image squared. This criterion is given by

$$(SNR)_p = \{[\text{peak of g}(i,j)]^2/rms\}^{1/2}, \tag{17}$$

where *rms* is given by Eq. (15) and the peak value is the total dynamic range of the decrypted image. Hence, (*SNR*)$_{rms}$ and (*SNR*)$_p$ differ by a scale constant equal to the ratio of maximum grey-level to average grey-level. To determine the robustness of the encryption, the *rms* is calculated for a decryption using an unknown random mask and the spatial frequency. The image of Fig. 5c is used to make the decryption to retrieve the original image. To do this, another random mask is created by computer to obtain a fringe pattern by means of Eq. (7). According to Fig. 5b, the result of the fringe pattern obtained is in correct, as shown in Fig. 7a. Also, the **HDM** is applied to retrieve the image from Fig. 7a. Using the correct spatial frequency f_o, the result obtained is shown in Fig. 7b. According to Fig. 5a, the original image cannot be observed. Using the pixels of Fig. 5a, pixels of Fig. 7b and Eq. (15), the error is determined. The result is a value *rms* =114.47 grey-levels. Figure 7c shows the result of applying the **HDM** using the incorrect frequency. Another one hundred and thirty six random masks created by computer were used to perform the decryption. The results obtained are shown in Fig. 7d. These results show that the original image cannot be observed on the screen. Therefore, the encryption has a great robustness. To determine the quality of the retrieved images, the *rms*, (*SNR*)$_{rms}$ and (*SNR*)$_p$ are calculated for a decryption using the correct random mask and the correct frequency f_o. Using the data of the original image of Fig. 5a and the data of retrieved image Fig. 5d, the *rms*, (*SNR*)$_{rms}$, and (*SNR*)$_p$ are calculated. The results are *rms* =4.6, (*SNR*)$_{rms}$ = 42.896 and (*SNR*)$_p$ = 7.298 grey-level. To describe the error between the histogram of the decrypted image and the original image, the *rms*$_h$ value is calculated. This value is described by the relation

$$rms_h = \sqrt{\frac{1}{n}\sum_{i=1}^{n}[h_d(i) - h_o(i)]^2}, \tag{18}$$

where $h_d(i)$ are data of the histogram of the decrypted image, $h_0(i)$ are the data of the histogram of the original image, and n is the number of grey-levels. Based on the histograms of Fig. 5e, the error between these two histograms is an *rms*$_h$ =10.936. The results for the retrieved image of Fig. 3f according to the original image Fig. 2a are a value *rms* = 4.35, (*SNR*)$_{rms}$ = 34.762, and (*SNR*)$_p$ = 7.571 grey-level. The changes in the grey-level, based on the histograms of Fig. 3g, have a value of *rms*$_h$ =10.124. Another image used for encryption and decryption is a dummy face, which is shown in Fig. 8a. The results of image encryption and decryption are shown in Figs. 8b and 8c, respectively. The quality of the retrieved image Fig. 8c according to the original image Fig. 8a has a value for *rms* = 4.2, (*SNR*)$_{rms}$ = 37.46 and (*SNR*)$_p$ = 6.982 grey-level. The variation in the grey-level of the decrypted image with respect to the original image is determined by means of histograms, which are shown in Fig. 8d. The error between these two histograms has a value of *rms*$_h$ =10.936. The last image used for encryption and decryption is a word, which is shown in Fig. 9a. The results of image encryption and decryption are shown in Figs. 9b and 9c, respectively. The quality of the retrieved image Fig. 9c according to the original image Fig. 9a has a value of *rms*=4.2, (*SNR*)$_{rms}$ = 34.24 and (*SNR*)$_p$=7.999 grey-level. The variation of the grey-level of the decrypted image with respect to the original image is determined by means of histograms, which are shown in Fig. 9d. The error between these two histograms has a value of *rms*$_h$ =1.973. The quality results show that the percentage of error according to the *rms*

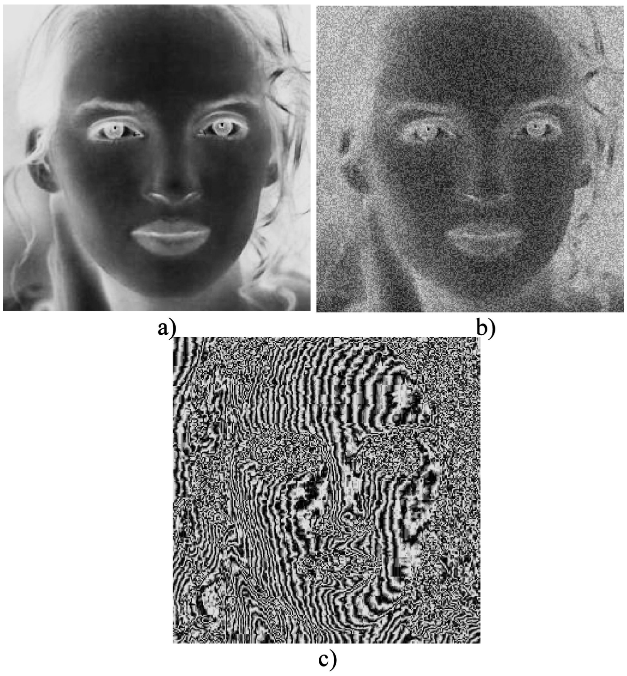

FIGURE 6. (a) Fringe patter with a frequency f_o with a period of 1 pixel; (b) Image of the random mask superimposed on fringe pattern Fig. 6a; and (c) Fringe pattern deformed with an image, whose values are normalized to 14π.

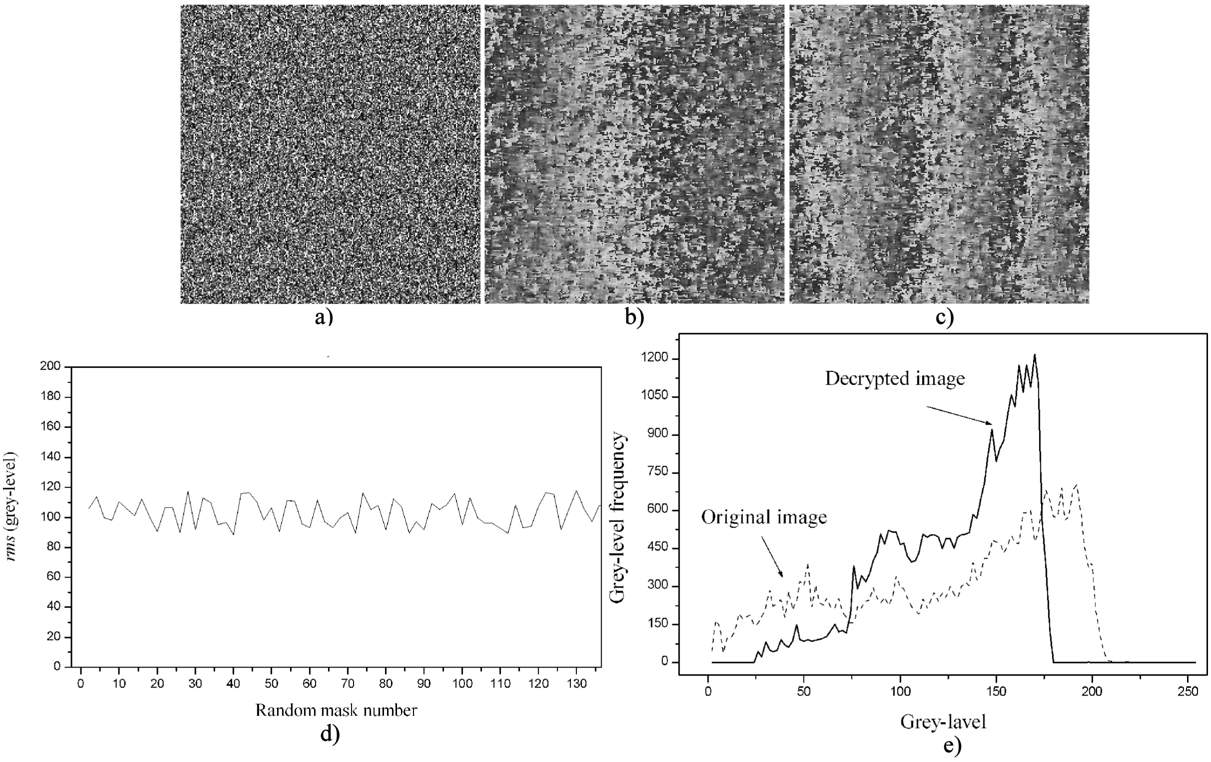

FIGURE 7. (a) Fringe pattern obtained by means of Eq.(8) using an unknown random mask; (b) Image retrieved from the fringe pattern of Fig.7(a) using the correct frequency f_o by means of the **HDM**; (c) Image retrieved from the fringe pattern of Fig.7(a), using unknown frequency f_o by means of the **HDM**; and (d) Error of the decrypted image using many unknown random mask and the **HDM**.

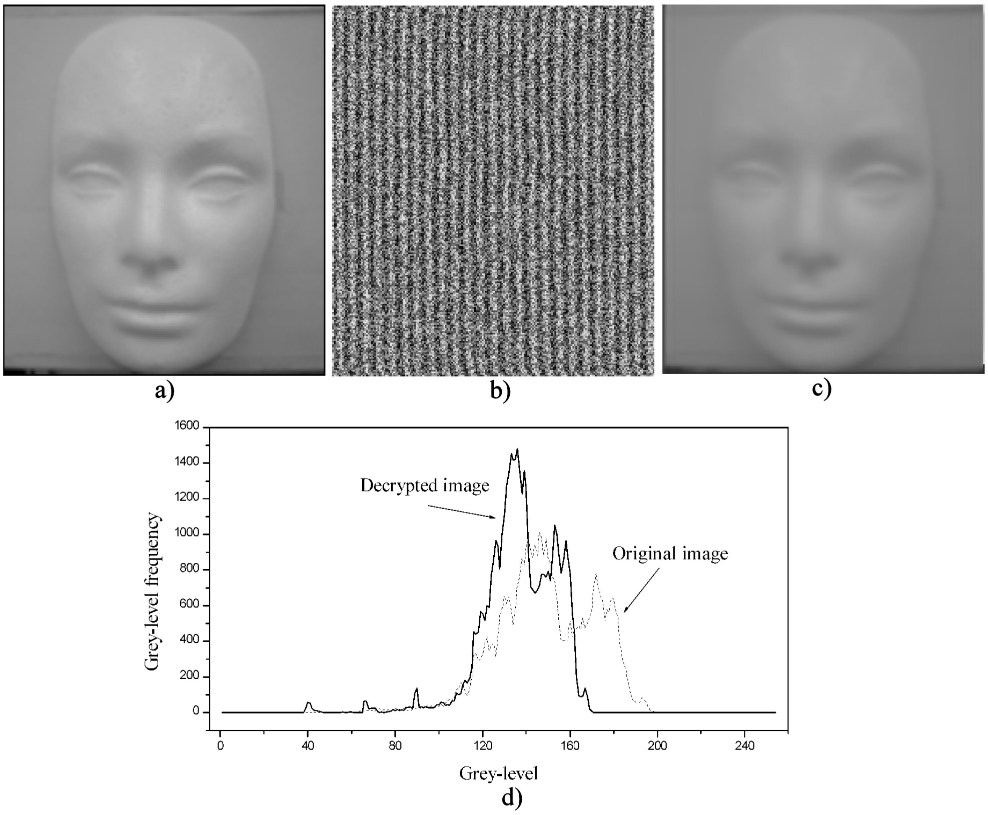

FIGURE 8. (a) Image of a dummy face used for encryption and decryption; (b) Encryption of Fig. 8a by means of the fringe pattern and the random mask; (c) Image decryption of Fig. 8b; and (d) Histograms of the decrypted image Fig. 8c and the original image Fig. 8a.

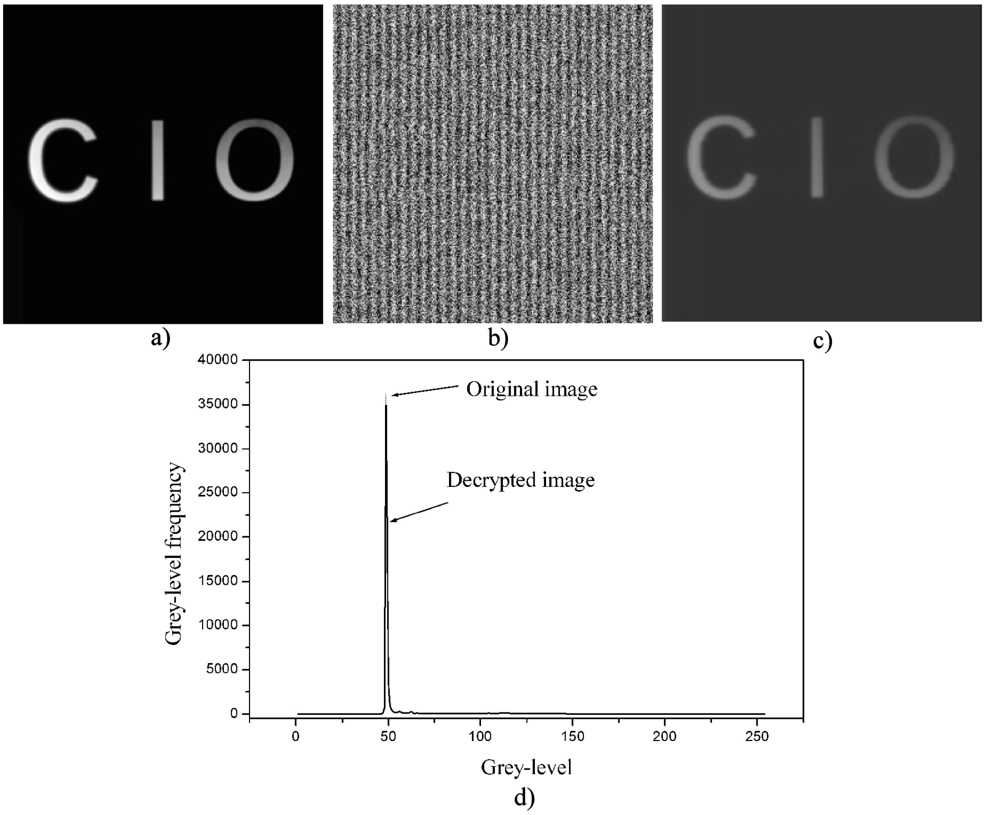

FIGURE 9. (a) A word used for encryption and decryption; (b) Encryption of Fig. 9a by means of the fringe pattern and the random mask; (c) Image decryption of Fig. 9b; and (d) Histograms of the decrypted image Fig. 9c and the original image Fig. 9a.

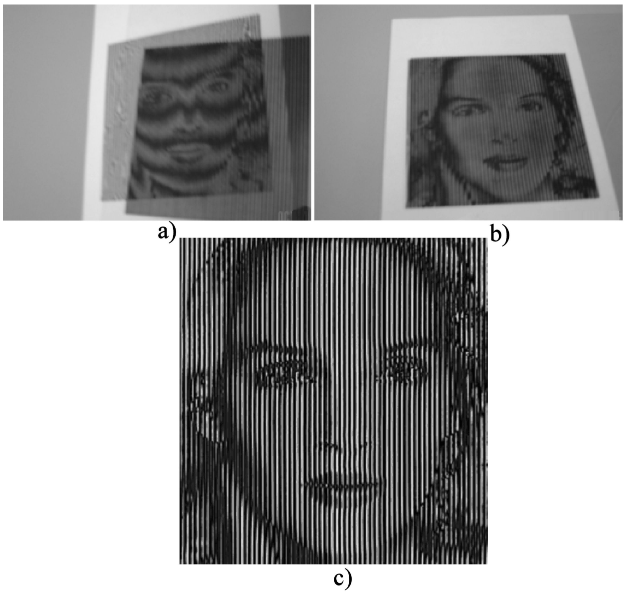

FIGURE 10. a) Superimposing a grating over the deformed fringe pattern; (b) Superimposing a grating over the deformed fringe pattern; and (c) Result of applying Eq.(8) in computational form.

and 256 grey-levels is around 1.8%. When the $(SNR)_{rms}$ is around 39, this value depends on the brightness of the image and the error of the decrypted image. When the $(SNR)_p$ is around 10, this value depends on the maximum of the decrypted image and the *rms* value. Based on the *rms* results obtained by other methods, the image retrieved by the technique described in this paper is good. It is shown by means of the error observed in other methods, which use similar images. The methods such as random phase-mask encoding, optical correlator, and spatial light modulator show percentage of error of over 5%. The percentage of error reported by the digital holography method is a 6.6%. The error percentage of reported by interferometric methods is 8%.

According to the quality criterion, high quality is as good an image as you desire [30]. The images decrypted by the technique described in this work are in agreement with this criterion. It can be proven by visual inspection and by computer vision. With respect to visual inspection, for the images decrypted by the described technique, the results are good. This means that the images decrypted by this technique can be recognized visually as the original image. Based on the results obtained, it is correct. With respect to the computer vision approach, the image is processed by means of pattern recognizing. Using the pattern intensity of the decrypted image, it can be achieved. In a comparison of the original image and the decrypted image, the only difference is a slight lack of smoothness in the decrypted image. Therefore, for recognition, it necessary to apply a smoothing to the original image. In this manner, the intensity pattern of the original image is equal to the intensity pattern of the decrypted image.

Hence, pattern recognition with a high level of similarity is possible. The main objective of a decrypted image in visual cryptography is to recognize it as the original image. Based on the result shown in this technique, this objective can be achieved by visual inspection or by computational recognition. The computer used in this process is a 1 GHz PC. Each image is encrypted in 0.004 sec and decrypted in .042 sec. To see the contribution of the processing time, the computational process is examined with respect to the processing time of the optical set-up. Based on the optical set-up of Fig. 1, the image encryption is carried out by projecting a grating and a random mask. It takes a least one second to switch on the light projectors to obtain the intensity pattern given by Eq. (4). By using Eq. (6), the image encryption is obtained in 0.004 see less time than that used by the optical set-up. For image decryption, the Eqs. (8) and (9) are examined. The multiplication of two intensity patterns can be obtained in optical form by superimposing these two intensity patterns [28]. Therefore, by superimposing a grating over the deformed fringe pattern, Eq. (8) is obtained. This procedure is shown by means of Figs. 10a and 10b. These figures show that at least one second is needed for superimposing the grating in the correct way to obtain the result given by Eq. (8), as shown in Fig. 10c. Therefore, the computational technique is faster than the optical set-up for performing the image encryption and decryption. Thus the technique for image encryption and decryption has been described. This computational encryption system has a good response for protecting data of the recovery trials of unauthorized users. This is because the key random mask and the phase detection algorithm are necessary for retrieving the original image. Otherwise it is impossible too see the original image. Therefore, the technique is a good security system for storing and exchanging image data electronically. Also, the retrieved images have good quality with respect to the original image.

5. Conclusions

A technique for image encryption and decryption based on phase encoding with a fringe pattern has been presented. The technique described here provides a valuable tool for sharing and storing image data electronically. This technique is a computational process whose algorithms are based on operations performed by an optical set-up for light projection technique. The image encryption is achieved with height robustness by means of the fringe pattern and the random mask. The image retrieved by the decryption has good quality and can be recognized as the original image. This technique is completely computational and optical devices are avoided. The performing real time for performing the image encryption and decryption is provided. Thus, this technique is performed with good repeatability in each image encryption and decryption.

Acknowledgments

The authors would like to thank the CONCYTEG, Guanajuato and CONACYT Mexico for their financial support.

1. P. Refregier and B. Javidi, *Opt. Lett.* **20** (1995) 767.
2. O. Matoba and B. Javidi, *Opt. Lett.* **24** (1999) 762.
3. H.T. Chang, W.C. Lu, and C.J. Kuo, *Appl. Opt.* **41** (2002) 4825.
4. S. Kishk and B. Javidi, *Appl. Opt.* **41** (2002) 5462.
5. B. Javidi and T. Nomura, *Opt. Lett.* **25** (2000) 28.
6. E. Tejahuerce and B. Javidi, *Appl. Opt.* **39** (2000) 6595.
7. O. Motoba and B. Javidi, *Opt. Lett.* **27** (2002) 321.
8. Y. Guo, Q. Huang, J. Du, and Y. Zhang, *Appl. Opt.* **40** (2002) 2860.
9. G. Unnikrishnan, J. Joseph, and K. Singh, *Opt. Lett.* **25** (2000) 887.
10. B. Zhu and S. Liu, *Opt. Commun.* **195** (2001) 371.
11. B. Hennelly and J.T. Sheridan, *Opt. Lett.* **28** (2003) 269.
12. J. Zhao, H. Lu, X. Song, J. Li, and Y. Ma, *Opt. Commun.* **249** (2005) 493.
13. L. Yu, X. Peng, and L. Cai, *Opt. Commun.* **203** (2002) 67.
14. X. Peng, L. Yu, and L. Cai, *Optics Express* **10** (2002) 41.
15. S.W. Han, C.S. Park, D.H. Ryu, and E.S. Kim, *Opt. Eng.* **38** (1999) 47.
16. B. Javidi, L. Bernard, and, N. Towgi, *Opt. Eng.* **38** (1999) 9.
17. L.Z. Cai, M.Z. He, Q. Liu, and X.L. Yang, *Appl. Opt.* **43** (2004) 3078.
18. M.Z. He, L.Z. Cai, Q. Liu, and X. L. Yang, *Appl. Opt.* **44** (2005) 2600.
19. M.Z. He, L.Z. Cai, X.C. Wang, and X.F. Meng, *Opt. Comm.* **247** (2005) 29.
20. G. Unnikrishnan, M. Pohit, and K. Singh, ‘ *Opt. Comm.* **185** (2000) 25.
21. C. Cheng and M Chen, *Opt. Commun.* **237** (2004) 45.
22. D. Malacara, M. Servin, and Z. Malacara, *Interferogram analysis for optical testing*, Marcel Dekker (Inc. U.S.A. 1998).
23. M. Naor and A. Shamir, *Advanced in Cryptography-Eurocrypt 94* **950** (1995) 1.
24. H. Yamamoto, Y. Hayasaki and N. Nishida, “*Securing information display by use of visual cryptography*”, Opt. Lett. Vol. 28 No. 17, 1564-1566 (2003).
25. M. Naor and A. Shamir, *Advanced in Cryptography-Eurocrypt 94* **950** (1995) 1.
26. H. Yamamoto, Y. Hayasaki, and N. Nishida, *Opt. Lett.* **28** (2003) 1564.

27. B. Jahne And H. Haubecker, *Computer vision and applications*, Academic Press, (U.S.A. 2000).

28. W.L. Wolfe, *Introduction to radiometry*, SPIE Optical Engineering Press, Vol. TT2, (1998).

29. P.H. Winston, *Artificial intelligence*, Addison-Wesley Publishing, (U.S.A. 1992).

30. D.W. Robinson and G.T. Reid, *Interferogram analysis: digital fringe pattern measurement techniques*, IOP Publishing, (U.K. 1993).

31. M. Servin, D. Malacara, and R. Rodríguez-Vera, *Appl. Opt.* **33** (1994) 2589.

32. R.C. Gonzalez and P. Wints, *Digital image processing*, Addison Wesley Publishing Company, (U.S.A. 1987).

33. K.R. Castleman, *Digital image processing*, Prentice Hall, (U.S.A 1996).