IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 23, 2018, accepted March 23, 2018, date of publication March 28, 2018, date of current version May 2, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2820603

Efficient Quantum Information Hiding for Remote Medical Image Sharing

AHMED A. ABD EL-LATIF[1], BASSEM ABD-EL-ATTY[1], M. SHAMIM HOSSAIN[2,3], (Senior Member, IEEE), MD. ABDUR RAHMAN[4], (Senior Member, IEEE), ATIF ALAMRI[2,3], AND B. B. GUPTA[5], (Senior Member, IEEE)

[1]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
[2]Chair of Pervasive and Mobile Computing, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[3]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[4]Department of Forensic Computing and Cyber Security, College of Computer Science and Information Technology, University of Prince Mugrin, Madinah 41499, Saudi Arabia
[5]National Institute of Technology Kurukshetra, Kurukshetra 136119, India

Corresponding author: M. Shamim Hossain (mshossain@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs, and also by the Al Bayan Foundation through the Scientific Research Unit of University of Prince Muqrin, Madinah.

ABSTRACT Information hiding aims to embed secret data into the multimedia, such as image, audio, video, and text. In this paper, two new quantum information hiding approaches are put forward. A quantum steganography approach is proposed to hide a quantum secret image into a quantum cover image. The quantum secret image is encrypted first using a controlled-NOT gate to demonstrate the security of the embedded data. The encrypted secret image is embedded into the quantum cover image using the two most and least significant qubits. In addition, a quantum image watermarking approach is presented to hide a quantum watermark gray image into a quantum carrier image. The quantum watermark image, which is scrambled by utilizing Arnold's cat map, is then embedded into the quantum carrier image using the two least and most significant qubits. Only the watermarked image and the key are sufficient to extract the embedded quantum watermark image. The proposed novelty has been illustrated using a scenario of sharing medical imagery between two remote hospitals. The simulation and analysis demonstrate that the two newly proposed approaches have excellent visual quality and high embedding capacity and security.

INDEX TERMS Medical images, quantum image processing, steganography, watermarking.

I. INTRODUCTION

Quantum information processing is a hot topic for researchers because information processing in quantum mechanics is more secure and efficient than that in classical information processing [1], [2]. Thus, it provides great technological contribution in communication, computation, cryptography, and image processing.

Quantum information is applied in image processing, wherein quantum parallelism is used to accelerate many image processing tasks such as quantum image steganography [3]–[7], quantum image encryption [8]–[10], and quantum watermarking [11]–[15]. The classical digital image should initially be transformed to quantum state using one of the quantum image representations to be operated by the quantum processing method. Various quantum representation models for digital images, such as Entangled Image [17], Qubit Lattice [18], flexible representation of quantum images [19], and novel enhanced quantum representation (NEQR) [20], have been presented in the literature [16]. Among the two proposed quantum data hiding approaches, the NEQR [20] representation model is utilized because it is extremely similar to classical image representation.

A. QUANTUM IMAGE STEGANOGRAPHY

Quantum image steganography is a concept that benefits from the merit of quantum image processing and that emerges from traditional steganography. Quantum steganography systems were originally presented by using the quantum information feature [3]. However, the proposed quantum steganography systems have the same security as the classical steganography system. The first model of quantum steganography, defined by extending the classical steganography, was proposed by

Natori [4]. Quantum steganography models can strictly be secured compared with the classical model.

In the quantum image steganography process, the quantum state of the obtained image is first encrypted, and then the encrypted version is embedded into the quantum cover image. Zhang *et al.* [6] proposed a quantum scheme based on the least significant qubit (LSQb) by utilizing the quantum Arnold image scrambling method during the encryption process before the quantum image is embedded into the quantum cover image. The proposed method has a payload capacity of 2-bit/8-bit. Miyake and Nakamae [14] scrambled the secret image by using the controlled SWAP gate in the encryption process at a payload capacity of 2-bit/8-bit. Naseri *et al.* [15] scrambled the secret image in the encryption process, where the LSQb and the most significant qubit (MSQb) are used in the data hiding process. Heidari and Farzadnia [7] employed the quantum Hilbert image scrambling technique to encrypt the quantum image. They adopted the Gray code during the embedding process. In [7] and [15], high PSNR value instead of the embedding capacity was pursued.

B. QUANTUM IMAGE WATERMARKING

Quantum watermarking utilizes quantum mechanical effects to realize quantum or classical information hiding tasks. Quantum watermarking based on image processing techniques uses a quantum image as carrier to hide quantum copyright information.

In 2013, Song *et al.* [11] designed a quantum image watermarking scheme based on quantum wavelet transformation. In the same year, Zhang *et al.* [12] presented a quantum watermarking scheme based on quantum Fourier transformation. A year later, Song *et al.* [13] presented another quantum image watermarking scheme based on Hadamard transformation. This scheme [11] utilizes a binary key to control Hadamard transform. In 2016, Miyake and Nakamae [14] presented the controlled-NOT operation-based quantum watermarking algorithm for the carrier and watermark images. This scheme was composed of three phases. The first phase is used to expand the watermark image with 8-bit and $2^{n-1} \times 2^{n-1}$ size to an image with 2-bit and $2^n \times 2^n$ size. The second phase is utilized to embed the expanded image by performing the controlled-NOT operation to the two LSQb of two images. The third phase is employed to extract the watermark with the original carrier image. The drawback of this scheme is evident in the third phase, where the extraction procedure requires the watermarked image, in addition to the original carrier image. In the same year, Zhang *et al.* [6] presented a quantum steganography scheme using the two LSQb to embed a $2^{n-1} \times 2^{n-1}$ secret image in an image measuring $2^n \times 2^n$.

In 2017, Naseri *et al.* [15] presented the LSB-based quantum image watermarking scheme that utilizes the XORing technique put forward by Kekre *et al.* [21]. Naseri *et al.* [15] aimed to embed a $2^{n-1} \times 2^{n-1}$ watermark image in a carrier image measuring $2^n \times 2^n$ with the LSQb and MSQb. Naseri's scheme uses the following two keys: the first one consists of the four MSQb of the watermark image, and the other one is generated during the embedding procedure. Thus, the proposed scheme embeds exactly half of the watermark image and not the total watermark; the other half becomes a key. The actual embedding capacity of Naseri's scheme is 1-bit per pixel, which differs from the suggested capacity of 2-bit per pixel.

C. CONTRIBUTION AND ORGANIZATION

Two efficient quantum information hiding schemes are proposed. A highly secure quantum image steganography scheme is proposed based on the logistic chaotic map. The classical image is first transformed into the quantum state using NEQR representation [20]. Results and analyses demonstrate that the presented quantum image steganography approach has good visual quality and high embedding capacity and security.

A quantum watermarking approach is also presented to hide a quantum gray image into a carrier image using two MSQb and three LSQb XORing techniques. The proposed scheme utilizes NEQR for quantum representation and quantum Arnold's cat map for simple representation to increase the security and capacity of the presented approach.

The remainder of this paper is organized as follows. A brief background on the Arnold image scrambling and the NEQR representation are provided in Section 2. The framework of the presented quantum hiding technique is illustrated using a scenario of securely sharing healthcare media in Section 3. The proposed quantum steganography approach is presented in Section 4. The proposed quantum watermarking approach is introduced in Section 5. The analysis and simulation results in terms of the payload capacity and visual quality of the proposed quantum steganography and watermarking schemes are presented in Sections 6 and 7, respectively. Finally, Section 8 draws the conclusions.

II. PRELIMINARY KNOWLEDGE

A. NEQR REPRESENTATION MODEL

The transformation process of an image from classical into quantum form is the first step in the quantum image processing. The gray-scale image can be represented in the quantum state by several models such as NEQR representation [20], which contains the color and corresponding position information of every pixel in the image. The representative expression of the NEQR model for a $2^n \times 2^n$ image can be expressed as follows:

$$|I\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes |i\rangle, |c_i\rangle = |c_i^{q-1} \ldots . c_i^1 c_i^0\rangle, c_i^k \in \{0, 1\}, \tag{1}$$

where $|c_i\rangle$ is the color value, and $|i\rangle$ is the information about the corresponding position. More information on NEQR representation is presented in [20].

B. LOGISTIC MAP

Chaotic maps play an important role in image encryption. Various chaotic maps, such as the logistic map, are available and can be defined as follows:

$$h_{i+1} = \delta h_i \left(1\text{-h}_i\right), \tag{2}$$

where $h_0 \in (0, 1)$ and $\delta \in (0, 4)$ are the control parameters of the logistic map.

C. ARNOLD IMAGE SCRAMBLING

The scrambling technique aims to transform an image from an intelligible into an unintelligible form through permutation of the positions of the pixels into new positions. One of the most widely used scrambling techniques is Arnold image scrambling, which can be defined as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod } N), \tag{3}$$

where N is the size of the image. The input includes x and y (position data of the pixels in the original image), and the output is the new position. The inverse of Arnold image scrambling can be defined as follows:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} (\text{mod } N). \tag{4}$$

III. HIGH-LEVEL FRAMEWORK OF THE PROPOSED QUANTUM HIDING OF HEALTHCARE MEDIA

Data protection for healthcare systems is a vital task [10], [22]–[25]. Figure 1 presents a framework for hiding quantum data for healthcare media in a smart city context. The framework is a scenario of sharing medical imagery between two remote hospitals in a smart city. Patients and healthcare staff from one place hide important medical Information (e.g. images) through the proposed quantum hiding technique and send public cover images to the cloud. The healthcare staff in another place accesses the images from the cloud, thereby recovering the content via the proposed detection/extraction procedures. The proposed quantum hiding technique ensures high confidentiality and security for patients and users of the healthcare system.

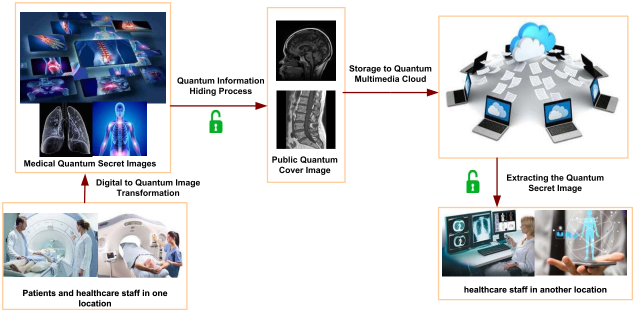
Medical Quantum Secret Images
Quantum Information Hiding Process
Public Quantum Cover Image
Storage to Quantum Multimedia Cloud
Digital to Quantum Image Transformation
Extracting the Quantum Secret Image
Patients and healthcare staff in one location
healthcare staff in another location

FIGURE 1. Proposed framework for hiding healthcare images.

IV. PROPOSED QUANTUM IMAGE STEGANOGRAPHY APPROACH

In this section, we illustrate how to embed a quantum secret image into a quantum image. During a pre-processing phase, each source secret image with 8-bit and $2^{n-1} \times 2^{n-1}$ size is first expanded to an image with 2-bit and $2^n \times 2^n$ size. The expanded image is then encrypted using quantum controlled-NOT gate controlled by a logistic map. The quantum encrypted image is embedded within the cover image that utilizes the two LSQb and MSQb for the quantum cover image. We assume that the $2^{n-1} \times 2^{n-1}$ secret image is expanded to $2^n \times 2^n$ size, and the size of the cover image is $|C\rangle$ is $2^n \times 2^n$. The embedding procedures of the presented approach are illustrated in Figure 2 and given by the following steps.

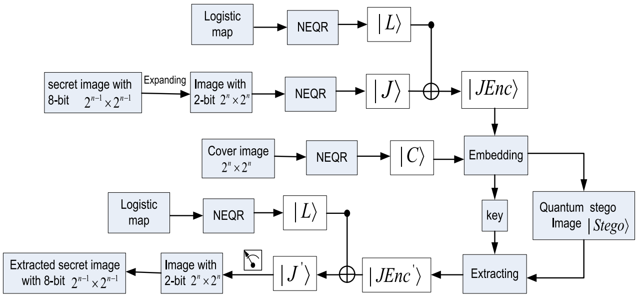
Logistic map
NEQR
$|L\rangle$
secret image with 8-bit $2^{n-1} \times 2^{n-1}$
Expanding
Image with 2-bit $2^n \times 2^n$
NEQR
$|J\rangle$
$|JEnc\rangle$
Cover image $2^n \times 2^n$
NEQR
$|C\rangle$
Embedding
Logistic map
NEQR
$|L\rangle$
key
Quantum stego Image $|Stego\rangle$
Extracted secret image with 8-bit $2^{n-1} \times 2^{n-1}$
Image with 2-bit $2^n \times 2^n$
$|J'\rangle$
$|JEnc'\rangle$
Extracting

FIGURE 2. Extracting and embedding procedures of the proposed quantum steganography approach.

Step 1: The secret gray-scale image with 8-bit and size of $2^{n-1} \times 2^{n-1}$ is expanded to the image with 2-bit and size of $2^n \times 2^n$.

Step 2: The cover image and the expanded secret image are transformed into quantum states as follows:

$$\begin{aligned} |C\rangle &= \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes |i\rangle, \\ |c_i\rangle &= |c_i^{q-1} \ldots . c_i^1 c_i^0\rangle, \, c_i^k \in \{0, 1\}; \end{aligned} \tag{5}$$

$$\begin{aligned} |J\rangle &= \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} |c_j\rangle \otimes |j\rangle, \\ |c_j\rangle &= |c_j^1 c_j^0\rangle, \, c_j^k \in \{0, 1\}. \end{aligned} \tag{6}$$

Step 3: Values for the control parameters h_i and δ are selected, where $h_0 \in (0, 1)$; $3.85 \leq \delta \leq 4$ to run the Logistic map, and $h_{i+1} = \delta h_i \left(1\text{-h}_i\right)$,

where I = 0, 1,…, 2^{2n}, ($2^{2n}$is the image size).

Step 4: The generated sequence $\{h_i\}$ is transformed into an integer sequence as follows:

$$h_i^* = |fix((h_i - fix(h_i)) \times 10^8)| mod\ 3. \tag{7}$$

Step 5: The sequences $\{x_i^*\}$ are transformed into the quantum state as quantum controlled-NOT image $|L\rangle$.

$$|L\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|c_j\rangle\otimes|j\rangle,$$
$$|c_j\rangle = |c_j^1 c_j^0\rangle,\ c_j^k\in\{0,1\}. \tag{8}$$

Step 6: The quantum secret image $|J\rangle$ is encrypted by performing the quantum controlled-NOT gate controlled by $|L\rangle$, as shown in Fig. 3.

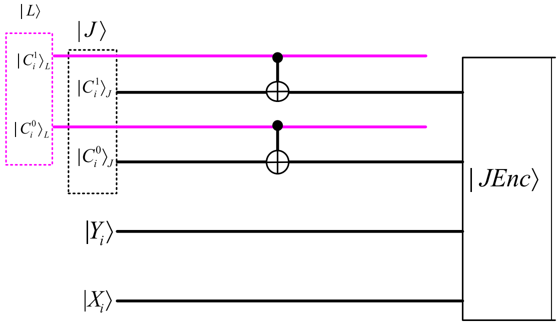

FIGURE 3. **Quantum circuit for the encryption process.**

Step 7: The first two MSQb and the first three LSQb XORing techniques are utilized to embed the encrypted quantum secret image $|JEnc\rangle$ into the quantum cover image $|C\rangle$, and a key $|K\rangle$ is generated from the embedding process, as illustrated in the following algorithm.

V. PROPOSED QUANTUM IMAGE WATERMARKING APPROACH

Here, we present the proposed quantum image watermarking approach. This scheme utilizes the Arnold's cat map to create confusion in the expanded watermark image $|W\rangle$. The procedure of the embedding processes of the proposed scheme is based on the two LSQb and MSQb of the cover image. Assume that the carrier image $|C\rangle$ with the size of $2^n\times 2^n$ and watermark image with the size of $2^{n-1}\times 2^{n-1}$ are expanded to $|W\rangle$ with the size of $2^n\times 2^n$. The embedding and extracting processes of the proposed scheme are shown in Figure 4 and given as follows.

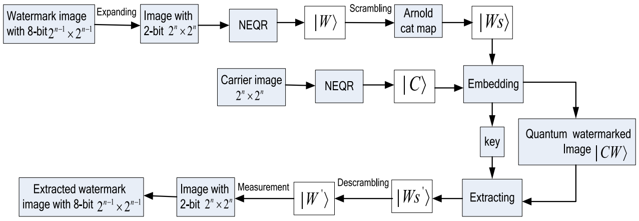
Watermark image with 8-bit $2^{n-1}\times 2^{n-1}$
Expanding
Image with 2-bit $2^n\times 2^n$
NEQR
$|W\rangle$
Scrambling
Arnold cat map
$|Ws\rangle$
Carrier image $2^n\times 2^n$
NEQR
$|C\rangle$
Embedding
key
Quantum watermarked Image $|CW\rangle$
Extracted watermark image with 8-bit $2^{n-1}\times 2^{n-1}$
Image with 2-bit $2^n\times 2^n$
Measurement
$|W'\rangle$
Descrambling
$|Ws'\rangle$
Extracting

FIGURE 4. **Embedding and extracting processes of the presented quantum watermarking approach.**

A. EMBEDDING PROCEDURES

The embedding procedures of the presented quantum image watermarking approach consist of three phases, as follows.

Algorithm 1 Embedding Algorithm for the Proposed Quantum Image Steganography Scheme

```
Input: $|C\rangle$ and $|JEnc\rangle$
Output: $|Stego\rangle$ and $|K\rangle$

$|Stego\rangle = |C\rangle$
for j=0 to $2^{2n}-1$
  if $|C_j^7\rangle = |JEnc_j^0\rangle$ then $|k_j^0\rangle = |1\rangle$
  else if $|C_j^0\rangle \oplus |C_j^2\rangle = |1\rangle$ then
    if $|JEnc_j^0\rangle = |0\rangle$then $|Stego_j^0\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}|C_j^0\rangle$ end if
  else if $|C_j^0\rangle \oplus |C_j^2\rangle = |0\rangle$ then
    if $|JEnc_j^0\rangle = |1\rangle$ then $|Stego_j^0\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}|C_j^0\rangle$
    end if
  end if
  if $|C_j^6\rangle = |JEnc_j^1\rangle$ then $|k_j^1\rangle = |1\rangle$
  else if $|C_j^1\rangle \oplus |C_j^2\rangle = |1\rangle$ then
    if $|JEnc_j^1\rangle = |0\rangle$ then $|Stego_j^1\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}|C_j^1\rangle$end if
else if $|C_j^1\rangle \oplus |C_j^2\rangle = |0\rangle$ then
      if $|JEnc_j^1\rangle = |1\rangle$ then $|Stego_j^1\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}|C_j^1\rangle$
      end if
    end if
end for
```

Phase 1 (Expanding the Watermark Image):

Step 1: The watermark image with 8-bit and size of $2^{n-1}\times 2^{n-1}$ is expanded to the image with 2-bit and size of $2^n\times 2^n$.

Step 2: The watermark image is presented after expanding the carrier image in the corresponding quantum states by the NEQR representations as follows:

$$|C\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle\otimes|i\rangle,$$
$$|c_i\rangle = |c_i^{q-1}\ldots.c_i^1 c_i^0\rangle,\ c_i^k\in\{0,1\}; \tag{9}$$
$$|W\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|c_j\rangle\otimes|j\rangle,$$
$$|c_j\rangle = |c_j^1 c_j^0\rangle,\ c_j^k\in\{0,1\}. \tag{10}$$

Phase 2 (Quantum Watermark Image Scrambling $|W\rangle$):

The quantum watermark image $|W\rangle$ is scrambled by the Arnold's cat map as follows:

$$|W_S\rangle = Sc(|W\rangle) = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|c_j\rangle\otimes Sc(|j\rangle). \tag{11}$$

$Sc(|i\rangle)$ can be defined according to Eq. (3) as follows:

$$Sc(|i\rangle) = Sc(|y\rangle|x\rangle) = Sc(|y\rangle)Sc(|x\rangle)$$

where

$$\mathrm{Sc}(|y\rangle) = |2\mathrm{y} + \mathrm{x}\rangle \bmod N$$
$$\mathrm{Sc}(|x\rangle) = |\mathrm{y} + \mathrm{x}\rangle \bmod N.$$

Phase 3 (Embedding Scrambled Image$|W_S\rangle$ ***into carrier image*** $|C\rangle$*):*

The quantum scrambled image $|W_S\rangle$ is embedded into the quantum carrier image $|C\rangle$ by utilizing the first three LSQb XORing techniques and the first two MSQb. A key $|K\rangle$ is generated from the embedding process. The embedding procedure can be driven as the following algorithm.

Algorithm 2 Embedding Algorithm for the Proposed Quantum Image Watermarking Scheme

```
Input:$|C\rangle$ and $|W_S\rangle$.
Output:$|CW\rangle$ and $|K\rangle$.

$|K\rangle = \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} |00\rangle \otimes |j\rangle$
$|CW\rangle = |C\rangle$
for $j = 0$ to $2^{2n} - 1$
  if $|C_j^7\rangle = |Ws_j^0\rangle$ then $|k_j^0\rangle = |1\rangle$
  else if $|C_j^0\rangle \oplus |C_j^2\rangle = |1\rangle$ then
    if $|Ws_j^0\rangle = |0\rangle$then$|CW_j^0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |C_j^0\rangle$
    end if
  else if $|C_j^0\rangle \oplus |C_j^2\rangle = |0\rangle$ then
    if $|Ws_j^0\rangle = |1\rangle$ then $|CW_j^0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |C_j^0\rangle$
    end if
  end if
if $|C_j^6\rangle = |Ws_j^1\rangle$ then $|k_j^1\rangle = |1\rangle$
else if $|C_j^1\rangle \oplus |C_j^2\rangle = |1\rangle$ then
    if $|Ws_j^1\rangle = |0\rangle$ then $|CW_j^1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |C_j^1\rangle$
    end if
else if $|C_j^1\rangle \oplus |C_j^2\rangle = |0\rangle$ then
    if $|Ws_j^1\rangle = |1\rangle$ then $|CW_j^1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |C_j^1\rangle$
    end if
  end if
end for
```

B. EXTRACTION PROCEDURES

The extraction procedures of the presented quantum image watermarking approach consist of the following three phases.

Phase 1 (Extracting Quantum Scrambled Image $|Ws^{'}\rangle$ ***from watermarked image*** $|CW\rangle$*):*

The quantum scrambled image $|W_S^{'}\rangle$ can be extracted from the quantum watermarked image $|CW\rangle$ by using only $|CW\rangle$ and the same key $|K\rangle$ generated during the embedding process. The extracting algorithm can be driven as follows.

Algorithm 3 The Extracting Algorithm for the Proposed Quantum Image Watermarking Scheme

```
Input:$|CW\rangle$ and $|K\rangle$.
Output:$|W_S^{'}\rangle$

$|Ws^{'}\rangle = \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} |00\rangle \otimes |j\rangle$
for j = 0 to $2^{2n} - 1$
      if $|k_j^0\rangle = |1\rangle$ then $|Ws_j^0\rangle = |CW_j^7\rangle$
      else if $|CW_j^0\rangle \oplus |CW_j^2\rangle = |1\rangle$ then $|Ws_j^0\rangle = |1\rangle$
      else if $|CW_j^0\rangle \oplus |CW_j^2\rangle = |0\rangle$ then $|Ws_j^0\rangle = |0\rangle$
      if $|k_j^1\rangle = |1\rangle$ then $|Ws_j^1\rangle = |CW_j^6\rangle$
      end if
      else if $|CW_j^1\rangle \oplus |CW_j^2\rangle = |1\rangle$ then $|Ws_j^1\rangle = |1\rangle$
      else if $|CW_j^1\rangle \oplus |CW_j^2\rangle = |0\rangle$ then $|Ws_j^1\rangle = |0\rangle$
      end if
end for
```

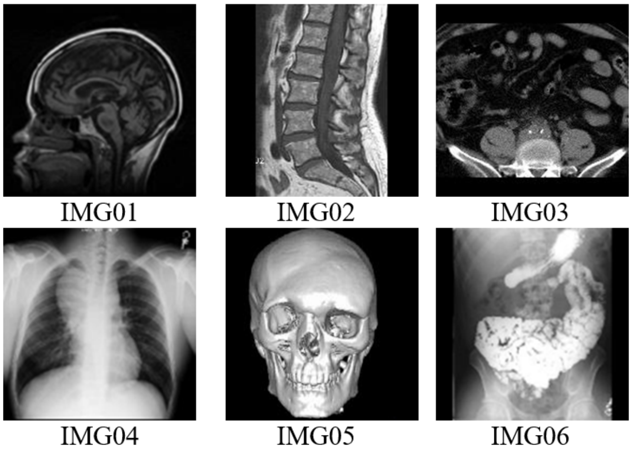

FIGURE 5. Cover and secret images for testing.

Phase 2 (Quantum Image $|Ws^{'}\rangle$ ***descrambling****):*

The quantum image $|Ws^{'}\rangle$ is descrambled as follows:

$$|W^{'}\rangle = Dc(|Ws^{'}\rangle) = \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} |c_j\rangle \otimes Dc(|j\rangle). \tag{12}$$

$Dc(|j\rangle)$ can be defined according to Eq. (4) as follows:

$$Ds(|j\rangle) = Ds(|y\rangle|x\rangle) = Ds(|y\rangle)Ds(|x\rangle)$$

where

$$\mathrm{Ds}(|y\rangle) = |\mathrm{y} - \mathrm{x}\rangle \bmod N$$
$$\mathrm{Ds}(|x\rangle) = |2\mathrm{x} - \mathrm{y}\rangle \bmod N$$

Phase 3(Measurement and Transformation of Quantum Watermark Image):

The transformation process of the extracted watermark image can be presented as follows:

Step 1: Quantum image $|W^{'}\rangle$ is measured to obtain a digital image with 2-bit and size of $2^n \times 2^n$.

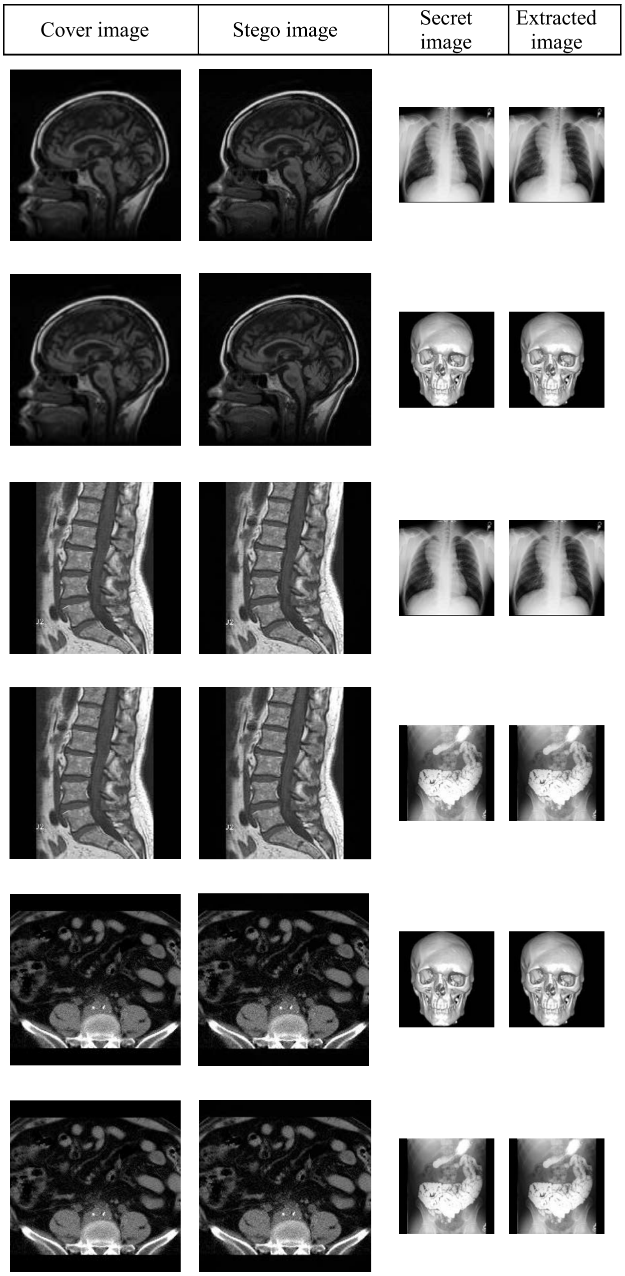

FIGURE 6. Visual effects of the proposed steganography scheme.

Step 2: The image with a size of $2^n \times 2^n$ and 2-bit is converted into the image with 8-bit and size of $2^{n-1} \times 2^{n-1}$.

VI. SIMULATION ANALYSIS OF THE PROPOSED QUANTUM IMAGE STEGANOGRAPHY SCHEME

To analyze the proposed approaches, a laptop with 6 GB RAM and Intel core i5-2450M CPU 2.50 GHz equipped with MATLAB R2017a (ver. 9.2.0.538062) is utilized to perform quantum operations on quantum images. IMG01, IMG02, and IMG03 images with the size of (256 × 256) are used as cover images, and IMG04, IMG05, and IMG06 images with the size of (128 × 128) as secret images (see Figure 5).

TABLE 1. PSNR (in dB) values for different images.

Cover image	Secret image	PSNR
IMG01	IMG04	46.2704
	IMG05	46.7901
	IMG06	46.2716
IMG02	IMG04	45.4560
	IMG05	46.7225
	IMG06	46.2056
IMG03	IMG04	46.2157
	IMG05	46.7670
	IMG06	46.5449

TABLE 2. Comparison with related schemes.

Schemes	Payload Capacity	Encrypt the secret image	PSNR value with Lena as cover image	Needs to extract the secret image
Our approach	2 bits/8 bits	quantum controlled-not image	46.3353	Control parameters to run the logistic map and the key matrix generated from the embedding process
Naseri *et al.* [15]	1 bit/8 bits	Scrambling the secret image	52.9641	The key matrix generated from the embedding process
Zhang *et al.* [6]	2 bits/8 bits	Quantum Arnold Image scrambling	43.1637	Only stego image
Miyake and Nakamae [14]	2 bits/8 bits	Scrambling the secret image by controlled SWAP gates	43.7936	The key used in the scrambling process in addition to the original carrier image
Heidari *et al.* [7]	2 bits/24 bits	Quantum Hilbert image scrambling	55.3456	The key matrix generated from the embedding process
Song *et al.* [11]	8bits/pixel	-	77.0482	The dynamic vector used in the embedding process in addition to the original carrier image

A. VISUAL QUALITY

The essential tool to evaluate the efficiency of the visual quality for any image steganography scheme is peak-signal-to-noise ratio (PSNR), which can be defined for two m × n images cover and stego as follows:

$$PSNR = 20\log_{10}(\frac{MAX_{Cover}}{\sqrt{MSE}}),$$

$$MSE = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}[Cover(x,y) - Stego(x,y)]^2. \qquad (13)$$

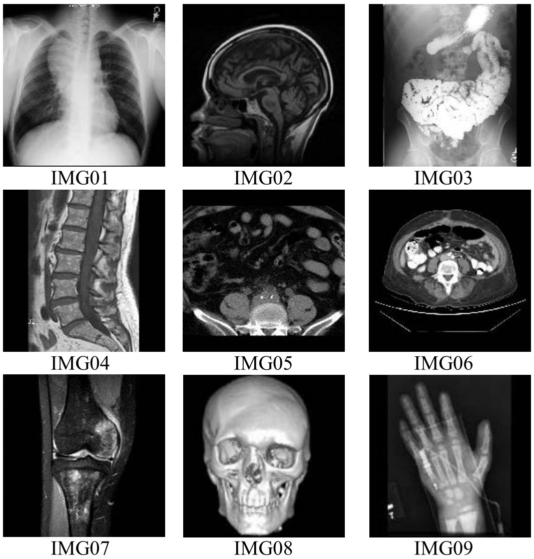

FIGURE 7. Carrier and watermark images for testing.

where MAX_{Cover} is the maximum pixel value of the cover image. The simulating results of the proposed scheme are shown in Figure 6 and Table 1 for the different images. The difference between the cover and stego images cannot be detected through the naked eye.

B. PAYLOAD CAPACITY

Embedding capacity is the proportion between the numbers of embedded bits to the number of cover bits. It can be represented as follows:

$$C = \frac{number\ of\ embedded\ bits}{number\ of\ cover\ image\ pixels} = \frac{2 \times n \times n\ bits}{n \times n\ pixel} = 2\text{-}bit/pixel. \quad (14)$$

The capacity of the presented quantum image steganography approach is 2-bit/pixel, which is sufficiently high.

C. SECURITY ANALYSIS

In our proposed scheme, we used two types of keys. The first one includes the control parameters (h_o, δ) to run the logistic map. The other one is the key matrix generated from the embedding process, whose size is equivalent to the size of the secret image. The approaches presented in [7] and [15] require secure communications to transmit the key matrix to demonstrate the security. However, in our scheme, the key matrix is used to increase visual quality, and the secret image is not secured. Table 2 shows that the presented quantum image steganography scheme has higher security than the other related quantum schemes with high capacity and acceptable visual quality.

VII. SIMULATION ANALYSIS OF THE PROPOSED QUANTUM IMAGE WATERMARKING SCHEME

IMG01, IMG02, IMG03, IMG04, IMG05, IMG06, and IMG07 images with the size of (256 × 256) are used as carrier images, and IMG08 and IMG09 images with the size of (128 × 128) as watermark images (see Figure 7).

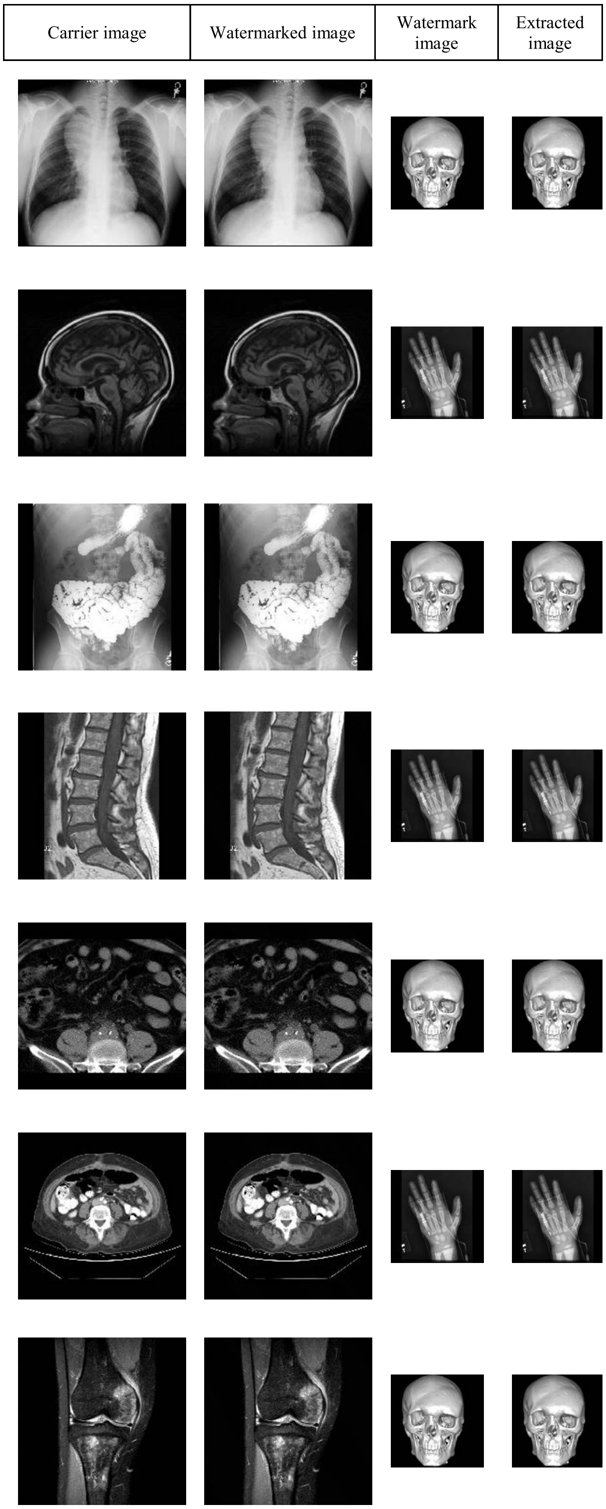

FIGURE 8. Visual effects of the proposed watermarking scheme.

A. PAYLOAD CAPACITY

Watermarking embedding capacity is the proportion between the numbers of embedded bits to the numbers of

TABLE 3. Visual effects of the proposed scheme.

Carrier image	Watermark image	PSNR
IMG01	IMG08	47.5552
	IMG09	47.1785
IMG02	IMG08	48.0998
	IMG09	48.1897
IMG03	IMG08	46.5937
	IMG09	46.5875
IMG04	IMG08	46.3696
	IMG09	46.5795
IMG05	IMG08	47.8346
	IMG09	47.8887
IMG06	IMG08	45.9205
	IMG09	46.3811
IMG07	IMG08	47.8133
	IMG09	48.0341

carrier pixels. The capacity of the presented approach is as follows:

$$C = \frac{number\ of\ embedded\ bits}{number\ of\ carrier\ image\ pixels} = \frac{2 \times n \times n\ bits}{n \times n\ pixel} = 2\text{-}bit/pixel \quad (15)$$

The capacity of the proposed quantum watermarking approach is 2-bit per pixel, which reveals the efficacy of the proposed approach.

B. VISUAL QUALITY

Figure 8 shows the simulation results of our scheme for different images, and the PSNR values between the watermarked and carrier images of the proposed scheme are shown in Table 3. As shown in Figure 8, the difference between the watermarked and carrier images cannot be detected by the naked eye. Table 3 demonstrates that the presented approach has sufficiently high PSNR values and height embedding capacity.

VIII. CONCLUSION

Two new and efficient information hiding approaches are presented based on MSQb and LSQb. A highly secure quantum image steganography approach is also shown. The security of the presented protocol lies on the encryption of the secret image with the controlled-"NOT" image, generated from the logistic map. The key matrix generated from the embedding process is used to increase the security in addition to its essential role to increase the visual quality. In the extraction process, control parameters are required to run the logistic map in addition to the key matrix. To provide the security, more keys or any information about the cover image or the secret image is required. In addition, the proposed quantum image steganography approach has high embedding capacity and acceptable visual quality.

A new quantum image watermarking approach is also introduced using the two MSQb and the XORing technique between the three LSQb. The proposed scheme utilizes the Arnold's cat map to create an incomprehensible watermark image before embedding it in the carrier image. The advantages of the presented approach include the following: only the watermarked image and the key are required to extract the watermark from the watermarked image, and the original carrier image is not required. Finally, the proposed scheme has excellent visibility and high embedding capacity.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Series on Information and the Natural Sciences). Cambridge, U.K.: Cambridge Univ. Press, 2000.

[2] B. Abd-El-Atty, S. E. Venegas-Andraca, and A. A. A. El-Latif, "Quantum information protocols for cryptography," in *Quantum Computing: An Environment for Intelligent Large Scale Real Application*. Cham, Switzerland: Springer, 2018, pp. 3–23.

[3] M. Curty and D. J. Santos, "Quantum steganography," in *Proc. 2nd Bielefeld Workshop Quantum Inf. Complex.*, 2000, pp. 12–14.

[4] S. Natori, "Why quantum steganography can be stronger than classical steganography," in *Quantum Computation and Information*. Berlin, Germany: Springer, 2006, pp. 235–240.

[5] B. Abd-El-Atty, A. A. A. El-Latif, and M. Amin, "New quantum image steganography scheme with Hadamard transformation," in *Proc. Int. Conf. Adv. Intell. Syst. Inform.*, 2016, pp. 342–352.

[6] T. Zhang, B. Abd-El-Atty, A. A. A. El-Latif, and M. Amin, "QISLSQb: A quantum image steganography scheme based on least significant qubit," in *Proc. Int. Conf. Math., Comput. Statist. Sci. Eng.*, 2016, pp. 40–45.

[7] S. Heidari and E. Farzadnia, "A novel quantum LSB-based steganography method using the Gray code for colored quantum images," *Quantum Inf. Process.*, vol. 16, p. 242, Oct. 2017.

[8] X.-H. Song, S. Wang, A. A. A. El-Latif, and X. M. Niu, "Quantum image encryption based on restricted geometric and color transformations," *Quantum Inf. Process.*, vol. 13, no. 8, pp. 1765–1787, 2014.

[9] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, "Quantum image encryption based on generalized Arnold transform and double random-phase encoding," *Quantum Inf. Process.*, vol. 14, no. 4, pp. 1193–1213, 2015.

[10] A. A. A. El-Latif, B. Abd-El-Atty, and M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, pp. 1073–1081, 2018, doi: 10.1109/ACCESS.2017.2777869.

[11] X.-H. Song, S. Wang, S. Liu, A. A. A. El-Latif, and X.-M. Niu, "A dynamic watermarking scheme for quantum images using quantum wavelet transform," *Quantum Inf. Process.*, vol. 12, no. 12, pp. 3689–3706, 2013.

[12] W.-W. Zhang, F. Gao, B. Liu, Q.-Y. Wen, and H. Chen, "A watermark strategy for quantum images based on quantum Fourier transform," *Quantum Inf. Process.*, vol. 12, no. 2, pp. 793–803, 2013.

[13] X. Song, S. Wang, A. A. A. El-Latif, and X. Niu, "Dynamic watermarking scheme for quantum images based on Hadamard transform," *Multimedia Syst.*, vol. 20, no. 4, pp. 379–388, 2014.

[14] S. Miyake and K. Nakamae, "A quantum watermarking scheme using simple and small-scale quantum circuits," *Quantum Inf. Process.*, vol. 15, no. 5, pp. 1849–1864, 2016.

[15] M. Naseri *et al.*, "A new secure quantum watermarking scheme," *Optik—Int. J. Light Electron Opt.*, vol. 139, pp. 77–86, Jun. 2017.

[16] F. Yan, A. M. Iliyasu, and S. E. Venegas-Andraca, "A survey of quantum image representations," *Quantum Inf. Process.*, vol. 15, no. 1, pp. 1–35, 2016.

[17] S. E. Venegas-Andraca and J. L. Ball, "Processing images in entangled quantum systems," *Quantum Inf. Process.*, vol. 9, no. 1, pp. 1–11, 2010.

[18] S. E. Venegas-Andraca and S. Bose, "Storing, processing, and retrieving an image using quantum mechanics," *Proc. SPIE*, vol. 5105, pp. 137–148, Aug. 2003.

[19] P. Q. Le, F. Dong, and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," *Quantum Inf. Process.*, vol. 10, no. 1, pp. 63–84, 2011.

[20] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "NEQR: A novel enhanced quantum representation of digital images," *Quantum Inf. Process.*, vol. 12, no. 8, pp. 2833–2860, 2013.

[21] H. B. Kekre, A. Athawale, and P. N. Halarnkar, "Increased capacity of information hiding in LSBs method for text and image," *Int. J. Elect., Comput. Syst. Eng.*, vol. 2, no. 4, pp. 246–249, 2008.

[22] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," *IEEE Syst. J.*, vol. 11, no. 1, pp. 118–127, Mar. 2017.

[23] M. S. Hossain, G. Muhammad, and A. Alamri, "Smart healthcare monitoring: A voice pathology detection paradigm for smart cities," *Multimedia Systems*. 2017, pp. 1–11. [Online]. Available: https://doi.org/10.1007/s00530-017-0561-x

[24] M. S. Hossain, "Patient state recognition system for healthcare using speech and facial expressions," *J. Med. Syst.*, vol. 40, no. 12, p. 272, 2016.

[25] L. Hu *et al.*, "Software defined healthcare networks," *IEEE Wireless Commun. Mag.*, vol. 22, no. 6, pp. 67–75, Jun. 2015.

AHMED A. ABD EL-LATIF received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2005 and 2010, respectively, and the Ph.D. degree in computer science and technology from the Harbin Institute of Technology, Harbin, China, in 2013. He is currently a Lecturer of computer science with Menoufia University. He has authored or co-authored many publications, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, and book chapters. He is a referee of many referred international repute journals and conferences. His areas of interests are multimedia content encryption, secure wireless communication, IoT, applied cryptanalysis, perceptual cryptography, secret media sharing, information hiding, biometrics, forensic analysis in digital images, and quantum information processing. He is a fellow at the Academy of Scientific Research and Technology, Egypt. He received many awards, including the State Encouragement Award in Engineering Sciences 2016, Arab Republic of Egypt, the Best Ph. D Student Award from the Harbin Institute of Technology, China, in 2013, and the Young scientific Award from Menoufia University in 2014.

BASSEM ABD-EL-ATTY was born in Menoufia, Egypt, in 1989. He received the B.S. degree in physics and computer science, and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2010 and 2017, respectively, where he is currently pursuing the Ph.D. degree in quantum information processing with the School of Mathematics and Computer Science, Faculty of Science. His research interests include quantum information processing and image processing.

M. SHAMIM HOSSAIN (SM'09) is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an adjunct Professor of EECS with the University of Ottawa, Canada. He has authored and co-authored approximately 170 publications, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. His research interests include cloud networking, social media, IoT, cloud and multimedia for healthcare, smart health, and resource provisioning for big data processing on media clouds. He is a member of the ACM and ACM SIGMM. He served as a member of the organizing and technical committees of several international conferences and workshops. He was a recipient of a number of awards including, the Best Conference Paper Award, the 2016 ACM Transactions on Multimedia Computing, Communications and Applications Nicolas D. Georganas Best Paper Award, and the Research in Excellence Award from King Saud University. He served as the Co-Chair, the General Chair, the Workshop Chair, the Publication Chair, and TPC for over 12 IEEE and ACM conferences and workshops. He is currently the Co-Chair of the first IEEE ICME Workshop on Multimedia Services and Tools for Smart-health MUST-SH 2018. He served on the Editorial Board of the IEEE MultiMedia, the IEEE Network, the IEEE Access, *Journal of Network and Computer Applications* (Elsevier), *Computers and Electrical Engineering* (Elsevier), *Games for Health Journal*, *Human-Centric Computing and Information Sciences and International* (Springer), and the *Journal of Multimedia Tools and Applications* (Springer). He was a Guest Editor of the IEEE Transactions on Information Technology in Biomedicine (currently JBHI), the *International Journal of Multimedia Tools and Applications* (Springer), *Cluster Computing* (Springer), *Future Generation Computer Systems* (Elsevier), *Computers and Electrical Engineering* (Elsevier), and the *International Journal of Distributed Sensor Networks*. He is currently a Lead Guest Editor of the *IEEE Communication Magazine*, the IEEE Transactions on Cloud Computing, the IEEE Access, *Future Generation Computer Systems* (Elsevier), and *Sensors* (MDPI).

MD. ABDUR RAHMAN (SM'18) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Canada, in 2011. He is currently an Assistant Professor with the Department of Forensic Computing and Cyber Security, University of Prince Mugrin (UPM), Madinah Al Munawwarah, Saudi Arabia. He is also the Chairman of the Computer Science and Forensic Computing and Cyber Security Department, UPM. He has authored and co-authored around 90 publications, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, and book chapters. He has seven U.S. patents and several are pending. His research interests include serious games, cloud and multimedia for healthcare, IoT, smart city, secure systems, multimedia big data, and next generation media. He has served as a member of the organizing and technical committees of several international conferences and workshops. He is a member of ACM. He has received over 12 million SAR as research grant. Recently, he received three best paper awards from the ACM and IEEE Conferences.

ATIF ALAMRI is currently an Associate Professor with the Information Systems Department, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. His research interests include multimedia-assisted health systems, ambient intelligence, and service-oriented architecture. He serves as a program committee member for many conferences in multimedia, virtual environments, and medical applications. He was a Co-Chair of the first IEEE International Workshop on Multimedia Services and Technologies for E-health, and the technical Program Co-Chair for the 10th IEEE International Symposium on Haptic Audio Visual Environments and Games. He was a Guest Editor of the IEEE Transactions on Instrumentation and Measurement.

B. B. GUPTA (SM'17) received the Ph.D. degree in information and cyber security from the Indian Institute of Technology Roorkee, India. He was a Visiting Researcher with Yamaguchi University, Japan, in 2015. He is currently guiding 10 students for their master's and Ph.D. research work in the area of information and cyber security. He has published over 90 research papers (including three books and 14 chapters) in international journals and conferences of high repute, including the IEEE, Elsevier, ACM, Springer, Wiley Inderscience, and so on. He has visited several countries, i.e., Canada, Japan, China, Malaysia, and Hong-Kong, to present his research work. His biography was selected and publishes in the 30th Edition of Marquis Who's Who in the World, 2012. He is also working principal investigator of various R&D projects. His research interest includes information security, cyber security, mobile security, cloud computing, Web security, intrusion detection, computer networks, and phishing. He has also served as a technical program committee member for over 20 International conferences worldwide. He is member of ACM, SIGCOMM, The Society of Digital Information and Wireless Communications, Internet Society, and the Institute of Nanotechnology, and a Life Member of the International Association of Engineers and the International Association of Computer Science and Information Technology. He is serving as an Associate Editor of the IEEE Access, an Associate Editor of IJICS, Inderscience and Executive Editor of IJITCA, Inderscience, respectively. He is also serving as a reviewer for the Journals of IEEE, Springer, Wiley, Taylor, and Francis. He is also serving as a guest editor for various reputed journals. He is also an editor of various international journals and magazines.