Hindawi
Complexity
Volume 2022, Article ID 3154650, 21 pages
https://doi.org/10.1155/2022/3154650

Research Article

DWT-SVD Based Watermarking for High-Resolution Medical Holographic Images

Fahrettin Horasan,[1] **Muhammed Ali Pala**,[2,3] **Ali Durdu**,[4] **Akif Akgül**,[5] **Ömer Faruk Akmeşe**,[5] **and Mustafa Zahid Yıldız**[2,3]

[1]*Department of Computer Engineering, Faculty of Engineering and Architecture, Kırıkkale Universityz, Yahşihan 71450, Kırıkkale, Turkey*
[2]*Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, Sakarya 54050, Turkey*
[3]*Biomedical Technologies Application and Research Center (BIYOTAM), Sakarya University of Applied Sciences, Sakarya, Turkey*
[4]*Department of Management Information Systems, Faculty of Political Sciences, Social Sciences University of Ankara, Altındag 06050, Ankara, Turkey*
[5]*Department of Computer Engineering, Faculty of Engineering, Hitit University, Corum 19030, Turkey*

Correspondence should be addressed to Muhammed Ali Pala; pala@subu.edu.tr

Received 19 February 2022; Revised 23 June 2022; Accepted 11 July 2022; Published 29 August 2022

Academic Editor: Ning Cai

Watermarking is one of the most common techniques used to protect data's authenticity, integrity, and security. The obfuscation in the frequency domain used in the watermarking method makes the watermarking stronger than the obfuscation in the spatial domain. It occupies an important place in watermarking works in imperceptibility, capacity, and robustness. Finding the optimal location to hide the watermarking is one of the most challenging tasks in these methods and affects the method's performance. In this article, sample identification information is processed with the method of watermaking on the hiding environment created by using a chaos-based random number generator on biomedical data to provide solutions to problems such as visual attack, identity theft, and information confusion. In order to obtain biomedical data, a lensless digital in-line holographic microscopy (DIHM) setup was designed, and holographic data of human blood and cancer cell lines, which are widely used in the laboratory environment, were obtained. The standard USAF 1951 target was used to evaluate the resolution of our imaging setup. Various QR codes were generated for medical sample identification, and the captured medical data were processed by watermarking it with chaos-based random number generators. A new method using chaos-based discrete wavelet transform (DWT) and singular value decomposition (SVD) has been developed and applied to high-resolution data to eliminate the problem of encrypted data being directly targeted by third-party attacks. The performance of the proposed new watermarking method has been demonstrated by various robustness and invisibility tests. Experimental results showed that the proposed scheme reached an average PSNR value of 564588 dB and SSIM value of 0.9972 against several geometric and destructive attacks, which means that the proposed method does not affect the image quality and also ensures the security of the watermarking information. The results of the proposed method have shown that it can be used efficiently in various fields.

1. Introduction

In recent years, significant developments in medical imaging technologies have brought many new perspectives to hospital and laboratory environments. These developments have resulted in large databases of information such as medical images, experimental procedure records, diagnostic and treatment reports, and patient records. The secure management, indexing, and archiving of these digitized data that emerged with these technologies become a significant issue. Illegal access, copying, and unlawful data modification cause serious security problems [1, 2]. A high degree of security procedures is required to store, record, and transmit these data securely. In addition, other identifying data attached to images may be lost, hacked, or archived incorrectly. Although various methods have been proposed in the literature to solve these problems, the watermarking technique is one of the most popular methods [3–5].

Watermarking is defined as embedding the data in another signal; it is embedding additional information directly into the data by gradually altering the original data or some transformed version of these data. The characteristics of a watermarking algorithm vary depending on the application for which it is designed. Undetectability, robustness, and security are essential criteria for a successful watermarking operation [6]. Undetectability defines the confidentiality of the presence of the watermark in the data, and the signal embedded in the data should not be noticed. The watermark embedded in the data must survive any reasonable action applied to the carrier. Otherwise, it is called fragile if it is not detected after the slightest change. In addition, embedded data should be resistant to unauthorized access and should not show any hint of the presence of the watermark. With the digital watermarking process, data corruption and access by unauthorized persons are highly restricted, producing results that are highly resistant to attacks [6–10]. In addition, a digital watermark is used to check for privacy, integrity, and malpractice obligations and tackle ethical and legal issues [11–13]. The watermarking of medical data brings with it various advantages. Thanks to the embedded data that contribute to savings in archiving large-scale digitized data. Embedded data reduce the need for additional bandwidth in transmission processes and increases the transfer rate. Thanks to the metadata hidden in the image data; it increases the safety of patients' records in the hospital and the safety of experiments in laboratory environments. This situation primarily provides advantages in archiving and proper classification and prevents unauthorized access to these data from outside [14, 15].

In recent years, many studies have been conducted on watermarking medical data. Alshaikn et al. [16] tried to determine the most suitable region to embed the watermark in the discrete cosine transform (DCT) based watermarking approach. They use a modified pigeon algorithm to determine the optimal burial path. Hsu et al. [17] proposed a high-capacity QR decomposition (QRD) based blind watermarking algorithm with artificial intelligence technologies for color images. Applying the watermark involves dividing the main image into nonoverlapping blocks of 4×4 pixels and then applying the QRD to each block. Ernawan et al. [18] proposed a self-embedded watermark using a spiral block mapping for tamper detection and restoration. They implemented a 3×3 block-based encoding, self-embedding watermark with two authentication bits and seven recovery bits. Muigai et al. [19] proposed an imperceptible and reversible medical image watermarking (MIW) scheme based on image segmentation, image estimation, and nonlinear difference broadening for the integrity and authenticity of medical images and detection of both intentional and unintentional manipulations.

Huang and Wu [20] proposed a new visual information hiding technique called optical watermarking for authenticating original printed documents. An optical watermark is a two-dimensional binary image. It can be of any shape and can be printed anywhere in a document. An optical watermark is created by overlaying many two-dimensional binary images, each of which has different carrier structural patterns that embed confidential information. The hidden information is embedded in each layer using phase modulation. Xie and Arce [21] developed a blind watermarking technique with a digital image signature for authentication. The signature algorithm is first implemented in the discrete wavelet transform (DWT) domain and then combined into the SPIHT compression algorithm. The capacity of the watermarking method is determined by the upper limit of the bit rate of information that can be hidden in the image using the binary engraving and multibit engraving methods. Arena et al. [22] proposed digital watermarks to validate both video and images. In such embodiments, the watermark is embedded in a master image, so that subsequent changes in the watermarked image can be detected with a high probability. The study presents the possibility of applying a real-time watermark on a video stream. Sidiropoulas et al. [23] proposed a new technique combining localization and reversibility. Moreover, the watermark dependency on the original image and the nonlinear watermark placement procedure ensured that no malicious attack would generate information leakage.

Thakkar et al. proposed a blind image watermarking scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD). This study applied DWT to the medical image's ROI (region of interest) to obtain different frequency subbands of wavelet decomposition [13]. Dhanalakshmi and Thaiyalnayaki proposed a binary watermarking method based on DWT-SVD and chaos cryptography [6]. A different spatial domain-based digital image watermarking method has been proposed by Lin et al. [24]. Today, encryption and watermarking methods have begun to work together to extend security to the electronic patient report (EPR) medical data [4]. An excellent watermarking algorithm must be robust and reliable against attacks [8]. Also, some studies have proposed the wavelet-based watermarking method for medical images [25–30].

In the SVD method, the diagonal elements of the singular value matrices are less subject to change against possible attacks after watermarking [31]. In more detail, the large-valued ones of the singular value matrix do not undergo significant change. In addition, the imperceptibility of the cover image is better as it allows for hiding less data belonging to the watermark. The most important advantage of using the DWT-SVD method is reducing the SVD process cost [32]. For this, the scaling feature of the DWT technique was used. R-DWT is applied to realize the most appropriate scaling. Thus, a robust, transparent, and less costly scheme is obtained [33]. The disadvantage of the SVD method is the false positive problem. This is the case when another watermark (actually another logo or image that is not watermarked) could be extracted from the watermarked image.

This study used chaos-based random number generators to counter the false positive problem. Watermarking is performed on randomly selected pixels. Thus, it is possible to remove the watermark only by those who know these chaotic keys.

This study developed a new method using chaos-based discrete wavelet transform (DWT) and singular value decomposition (SVD) for watermarking with high imperceptibility and robustness. In addition, a new application area has been gained by applying the proposed method to the data obtained from the DIHM system. In the following sections of this article, the theoretical details of holography and the design parameters of our microscopy setup are explained in detail. The standard USAF 1951 target was used to evaluate the resolution of the imaging setup. Human blood and cancer cell culture cells, which are widely investigated in clinical and laboratory applications, were used as medical samples. A QR code was created for information such as medical sample preparation procedures and patient information. The chaotic system is used for random number generators. The dynamic analysis results of the chaotic system determined as suitable for the watermarking process are shown. The randomness performance of random number generators has been demonstrated by NIST and ENT statistical tests. The new method using discrete wavelet transform (DWT) and singular value decomposition (SVD) intended for watermarking is explained in detail. The performance of the proposed new watermarking method has been demonstrated by various robustness and invisibility tests.

2. Lensless Digital In-Line Holographic Microscopy

Microscopy systems that allow imaging at the micro-nano level have an undeniable effect on the development of today's scientific world. Micro-nano level sensors developed based on semiconductor technology have expanded the usage area of microscopy systems and caused this development to progress. With these developments, DIHM has begun to be used in many application areas, from physics to medical imaging [34–37]. With its advantages such as wide field of view, high spatial resolution, easy integration, and low cost, DIHM has become a tool that performs essential functions, especially in the laboratory and clinical stages of medical imaging. DIHM is used in laboratory conditions to imaging microorganisms such as cancer cells, bacteria, yeast cells, or sperm cells, perform viability analyses, track the cells in 2D, and determine sample 3D localizations [38–42]. It is used in the clinic for human-level counting and classifying blood cells, morphological examination of medical samples, and disease diagnosis [43–45]. Considering all these areas of use, the commercial studies of DIHM systems are currently used for clinical and laboratory experiments. With DIHM, where algorithm integration is easy, various analyses can be obtained with high accuracy rates with traditional image processing methods, segmentation methods, or deep neural network methods [46, 47]. This situation constitutes an excellent alternative to the methods accepted as a gold standard, and it seems likely to reach more areas of use in the future. In this section, the basic principles of holography are mentioned, and the design parameters of our imaging system are detailed.

2.1. Hologram Theory. DIHM is based on Gabor's holographic principle [48]. The interaction of the light source and the rays emanating from this light source with the sample and the diffraction patterns resulting from this interaction are recorded by charge-matched semiconductors (CCD) or complementary metal oxide semiconductors (CMOS). The interaction of the beams emitted from the light source with the sample and the diffraction patterns resulting from this interaction are recorded via charge-coupled devices (CCD) or complementary metal oxide semiconductors (CMOS) [49]. Coherent sources are used as light sources, and spatially filtered light-emitting diodes (LED) are used in many applications in the literature [38, 50]. DIHM, in which no optical lens is used, uses Fourier optics' principles numerically in its image creation processes. According to the in-line principle, the hologram $(H(x, y))$ can be expressed as

$$\begin{aligned} H(x, y) &= |I(x, y)|^2 = |R(x, y)|^2 + |O(x, y)|^2 \\ &\quad + R^*(x, y)O(x, y) + O^*(x, y)R(x, y), \end{aligned} \tag{1}$$

where $|I(x, y)|^2$ is the diffraction image, $R(x, y)$ is the reference wave, $O(x, y)$ is the diffraction of the object, $R(x, y)^2$ the intensity of the reference wave (constant term), and $O(x, y)^2$ is the zero-order diffraction of the object and is very small compared to other terms, so that it can be neglected. $R^*(x, y)O(x, y)$ is the real image and $O^*(x, y)R(x, y)$ is the twin image. The hologram needs to be normalized [51]. For this, the constant DC ($|R(x, y)|^2 \cong |R(x, y)|^2 + |O(x, y)|^2$) term in (1) can be extracted from the hologram intensity data by recording between the sensor and the object plane without an object. It can be normalized with the average intensity value of the background of the hologram data. Normalization or background removal eliminates the inhomogeneous light distribution or unwanted noise in the hologram. In addition, the obtained hologram data can be obtained regardless of the reference wave or the imaging sensor's sensitivity [52]. Therefore, the hologram's real image and twin image terms must remain in the equation to obtain the object information. Thus, the result of background normalization is

$$\begin{aligned} \widetilde{H}(x, y) &= \frac{|I(x, y)|^2}{|R(x, y)|^2} \\ &\cong 1 + \frac{R^*(x, y)O(x, y) + O^*(x, y)R(x, y)}{|R(x, y)|^2}. \end{aligned} \tag{2}$$

2.2. Microscopy Setup and Imaging Evaluation. Our DIHM setup consists of a light source, pinhole, imaging sensor, and electronic components. All mechanical parts were 3D printed, and electronic components were controlled with a microcomputer. Due to the diffraction phenomenon, short-wavelength illumination sources can achieve higher spatial resolution [53]. For this reason, a Power LED source of 430 nm wavelength has been used as the light source. The power LED source was driven with a 250 mA constant current source. The microcomputer provides the PWM signal to coordinate the light source with the imaging sensor during hologram acquisition. With the PWM control, the heating of the light source is prevented, and therefore the temperature-dependent change of the wavelength is prevented. A 150 μm diameter laser cut pinhole was placed in front of the LED source to provide spatial filtering and make the light source partially coherent. Sony IMX 219PQ was used as the imaging sensor. The CMOS sensor has a maximum resolution of 3280 × 2464 and a pixel pitch is 1.12 μm. The imaging sensor has an approximately 10mm^2 active sensor area, which is equal to the field of view of the DIHM. All data obtained during the study were collected and processed at this resolution. The medical samples and the calibration slide were placed directly on the imaging sensor. The imaging sensor was connected to the microcomputer with the help of a flex cable, and parameters such as exposure time, gain, and white balance were adjusted. Considering the magnification factor in the produced imaging system, the distance between the sensor and the object (z_2) was chosen as less than 1 cm, and the distance between the imaging sensor and the light source (z_1) was chosen as 6 cm. Figure 1 shows a schematic representation of the DIHM system.

After the light source interacts with the object plane, the interference of the object's diffraction waves and reference waves on the imaging sensor generate the hologram. The hologram and background images collected with the help of the microcomputer were recorded as color images and then transferred to the PC to perform the image processing steps. Since the imaging sensor has a Bayer filter, only the green channel is used to obtain maximum light information. Background data were extracted from the hologram, and images were converted to [0, 255] scale. The normalized hologram data is backpropagated in the z optical axis between the sensor and object planes via the angular spectrum method [47, 54]. The angular spectrum method uses no approximations and is appropriate for small z_2 distances [55]. Fast Fourier transform (FFT) first transferred the hologram to the spatial frequency domain. Then, the hologram in the frequency domain is multiplied by the created transfer function. Finally, the images that have been multiplied in the frequency domain are converted to the spatial domain by inverse fast Fourier transform (IFFT). The angular spectrum method used in creating the transfer function can be mathematically expressed as follows:

$$I(x, y; z) = \mathfrak{I}^{-1}\left\{\mathfrak{I}\{I(x, y; 0)\}\exp\left\{i\frac{2\pi z}{\lambda}\sqrt{1-(\lambda f_x)^2-(\lambda f_y)^2}\right\}\right\}, \tag{3}$$

where $\mathfrak{I}$ represents the FFT and $\mathfrak{I}^{-1}$ represents the IFFT. x and y are the spatial coordinates in the image plane, z is the propagation distance, f_x and f_y represent th spectral coordinates in the Fourier space, and λ is the wavelength. $I(x, y; 0)$ is the expression of the hologram's light-intensity field on the imaging sensor and $I(x, y; z)$ the reconstructed image in the optic axis direction.

When creating the transfer function, the distance between the required image sensor and the sample may not be known in some cases. In order to solve this problem, it must be solved numerically by multiplying the transfer function formed from a small reconstruction distance with the hologram. In the study, 50 transfer functions were created with a 10 μm step size, multiplied with a hologram, and the sample images were obtained. Tenenbaum gradient, Brenner gradient, and Tamura gradient of all images were calculated to find the optimum distance through the images [56, 57]. The local maximum values of the calculated functions are taken as the best image. In order to improve the hologram images, methods such as phase retrieval and twin image elimination can be applied to images [58, 59]. However, in this study, these routines were not applied within the scope of the study, and the basic system microscopy scheme was considered.

The standard USAF 1951 resolution target was used to evaluate the resolution capability of our microscopy setup. USAF 1951 target has a maximum of seven groups and six elements. The raw hologram obtained by USAF 1951 is shown in Figure 2(a), the region of interest (ROI) is shown in Figure 2(a), the image resulting from the reconstruction of the ROI is shown in Figure 2(c), and the group is shown in Figure 2(d), the normalized pixel intensity value of group 7 and elements 6 is given. The figures show that the microscope designed for imaging resolves 228.1 (lp/mm).

2.3. Sample Preparation and Data Collection. As for medical data, the most analyzed medical samples in clinics and laboratories were preferred. Human blood cells were imaged as the first medical sample. The sample blood samples used in this study were approved by the Sakarya University Ethics Committee's decision number 050.01.04/291. The participant was healthy laboratory personnel, verbal and written information was given about the study, and the samples were used with permission. Blood samples were prepared in 5 μL, and the samples were placed on a glass slide. MCF-7 breast cancer cell culture was used as a secondary medical sample, and MCF-7 cell culture is one of the most frequently used cell cultures in laboratory research. The MCF-7 cell line was supported and grew with 10% fetal bovine serum and 1% penicillin and incubated at 37°C with 5% CO$_2$. Trypan blue was added to the cells in a ratio of 1 : 1. It was taken in the same volume as the blood sample and imaged in DIHM. In Figure 3, images of the obtained medical samples and regions of interest are given.

3. The Used Chaotic System, Its Dynamic Analysis, and RNG Design

Edward Lorenz introduced the concept of chaos and the attractor, which is very sensitive to initial conditions, in 1963 [60]. In recent years, developments related to chaotic systems have attracted the attention of researchers [61, 62]. The science of chaos, briefly defined as the order in disorder, is encountered in many applications such as electronics,

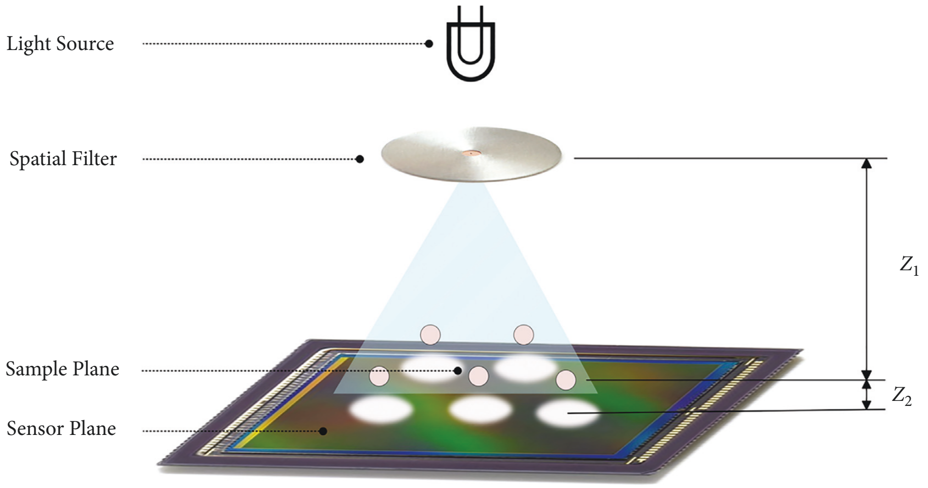
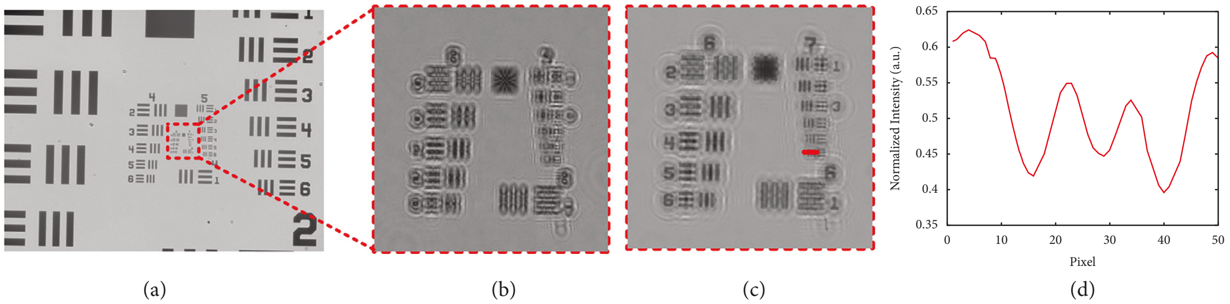
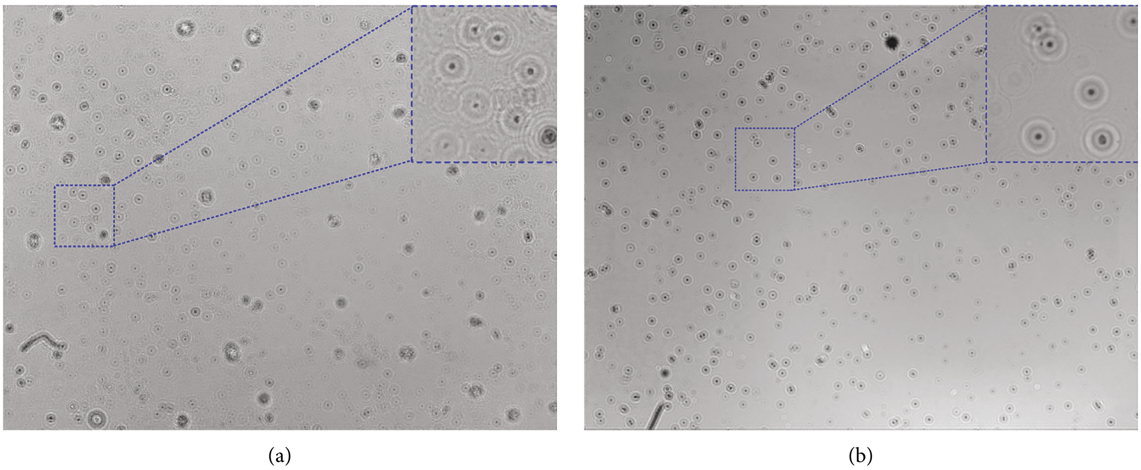


Figure 1: Schematic representation of the DIHM system, z_2 distance less than 1 cm and z_1 distance 6 cm.



(a) (b) (c) (d)

Figure 2: Resolution evaluation of the imaging system: (a) raw hologram data obtained in size 3280 × 2464; (b) the raw hologram of the target region of interest; (c) reconstructed hologram; (d) normalized intensity profile of group 7 element 6.



(a) (b)

Figure 3: Medical samples were obtained with DIHM. (a) Image of human blood cells and selected ROI. (b) MCF-7 cell line and selected ROI.

computers, control, finance, and health because it is mathematically simple and can be used in practice [63–67].

This section discusses the fundamental dynamic analysis of the chaotic system without equilibrium points used for watermarking. The chaos-based random generator will form the basis of watermarking work and its statistical tests. The equations for the chaotic system without equilibrium points used for the chaos-based random number generator are

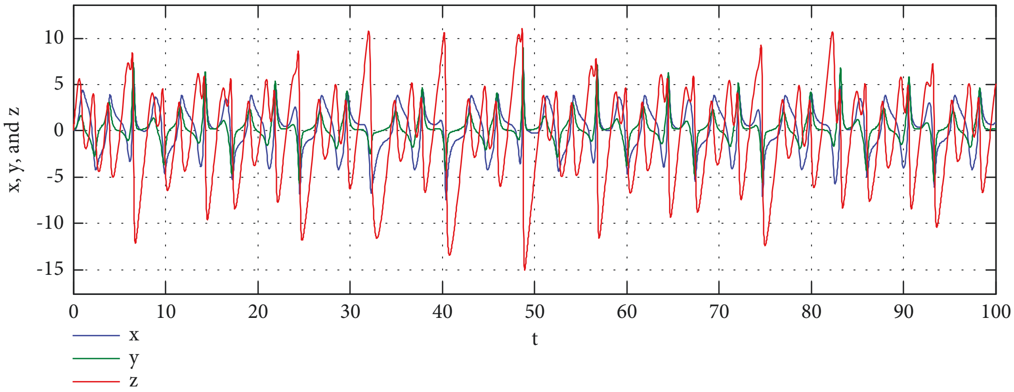


Figure 4: Time series for x, y, and z outputs.

$$\begin{aligned}\dot{x} &= ay - x + zy,\\ \dot{y} &= -bxz - cx + yz + d,\\ \dot{z} &= e - fxy - x^2.\end{aligned} \tag{4}$$

The random numbers required for the watermarking application are generated from chaotic systems. 3D continuous-time chaotic system has six parameters. The values of these parameters are $a = 2.8, b = 0.2, c = 1.4, d = 1, e = 10,$ and $f = 2$. In addition, the initial conditions of the chaotic system are $x(0) = 0, y(0) = 0, z(0) = 0$. In other cases, the system may emerge from chaos. In (5), the set of equations can be seen with parameter values entered. The watermarking application generated random numbers according to the parameter values and initial conditions selected in the article study. In order to show that the system is chaotic, some analyzes are given in the article and it is shown that the system is chaotic. With the system that proved to be chaotic, random number generation was made as given in algorithm 1, and the watermarking application was carried out as a result of successful test processes.

$$\begin{aligned}\dot{x} &= 2.8y - x + zy,\\ \dot{y} &= -0.2xz - 1.4x + yz + 1,\\ \dot{z} &= 10 - 2xy - x^2.\end{aligned} \tag{5}$$

3.1. Dynamic Analysis. The time series analysis, sensitivity to initial conditions, and phase portraits of the chaotic system used in the article are shown in Figures 4–6. The sensitivity analysis of the initial conditions shows that the system exhibits different behavior with a minimal change. For this reason, the chosen chaotic system is suitable for essential studies such as encryption, data hiding, and watermarking.

3.2. Random Number Generation. Random numbers are generally divided into pseudo (PRNG) and true (TRNG). If we obtain different random numbers every time we start a system, this system is called TRNG. Because of the production of different random numbers each time, the use of TRNG is, in some cases, not suitable for studies such as encryption. For this reason, PRNG *s* can be preferred to get the same numbers when the system is started from the beginning. In this article, pseudorandom numbers were preferred because the same random numbers were needed when the system was rerun for the watermarking application. The pseudocode for how random numbers are generated is given in Algorithm 1.

If Algorithm 1 is explained, a chaotic system without an equilibrium point selected for the PRNG design is discretized by the RK4 numerical analysis algorithm since it is a continuous-time system. After the discretization process, the obtained point-based numbers were converted to a binary number system. After the conversion process, a 32 bit binary number system is produced for each point-based number. This study created random number sequences by selecting low-significant 16 bit number series from the 32nd bit to the 17th bit of each generated number.

3.3. Statistical Tests. NIST-800-22 statistical tests with the highest standards at the international level were used to measure the randomness performance of the numbers produced. Although the NIST-800-22 tests consist of 16 different tests, a series of numbers consisting of a minimum of 1 Mbit “0” and “1” is required. If one or more NIST-800-22 tests fail, the bit series must be rebuilt and the test repeated. All tests must be successful for the produced series of bits to be successful. The NIST-800-22 Test results are interpreted according to *P* values. The result must be greater than the defined *P*-value for the test to be considered successful. The random bit series created successfully passed this study’s NIST-800-22 statistical tests. The chosen chaotic system is three-dimensional. Therefore, three different outputs can be obtained: *x*, *y*, and *z*. However, in this study, the tests were performed only with random numbers obtained from the output “*x*” and the results are given in Table 1.

According to Table 1, all *P* values are greater than 0.001. Therefore, the generated random bit series has successfully passed all NIST-800-22 statistical tests. Generated random numbers can be safely used in encryption, data hiding, and watermarking applications due to the test’s success.

Another reliable statistical test, the ENT test, is a test application developed by John Walker that applies various

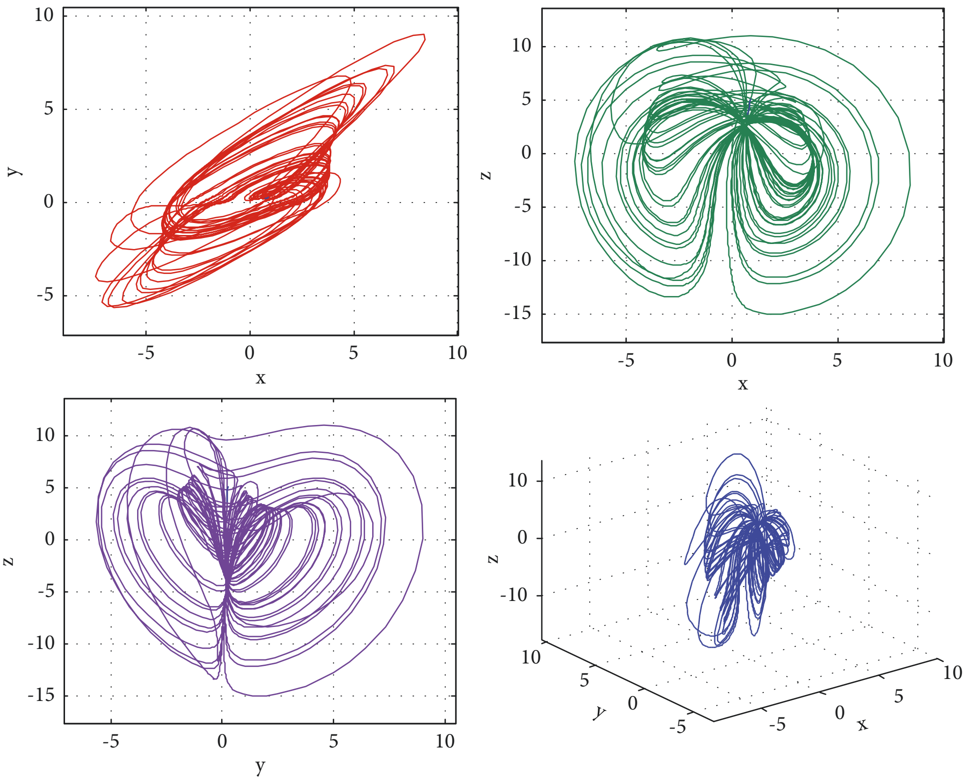


FIGURE 5: Phase portraits for x-y, x-z, y-z, and x-y-z.

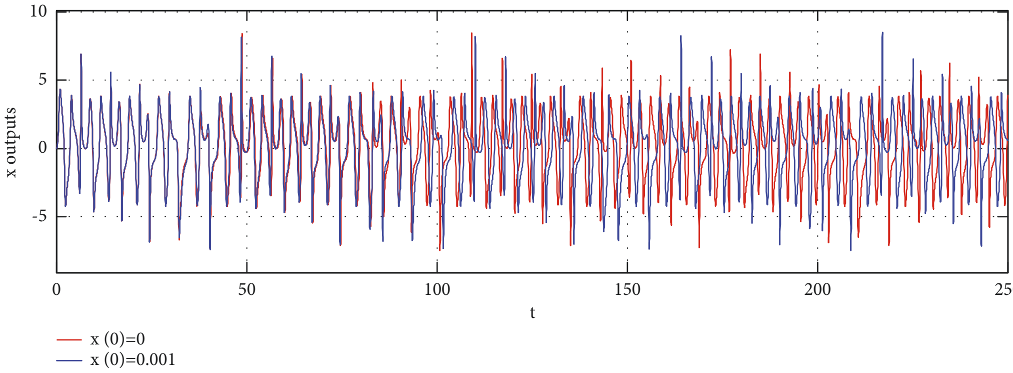


FIGURE 6: Sensitivity to initial conditions for x output.

tests to byte sequences produced by pseudorandom number generator applications [25]. There are five different statistical tests found in the ENT test that define the randomness of bit sequences. ENT test results mean values of random numbers obtained from output x are given in Table 2. According to Table 2, it was concluded that the random numbers generated from the last 16 bit values of the x output, which passed all tests, provided randomness.

4. DWT-SVD Based Watermarking Application

This section describes watermarking the cover image and removing the watermark from the watermarked image. First, a 256×256 dimensional matrix (selected blocks) is obtained from the high-resolution medical images of blood and cancer cells through chaos-based random numbers. In other words, it forms the $B \in R^{M \times M}$ matrix, we call selected blocks, which consists of randomly selected pixels that we obtained from the large-size image we call cover image (C). R-level wavelet transform algorithm is applied to this obtained image. The watermarking process uses singular value decomposition (SVD) for the $M \times M$ size image to be watermarked and the $N \times N$ size watermark. In the continuation of this section, details of the discrete wavelet transform, singular value decomposition, and watermarking algorithm are given.

4.1. Generating Selected Blocks Matrix from Cover/Watermarked Cover Image.

This study hides the watermark in the B matrix created from the pixels selected with CBRNG from the original image. Then, this matrix with a watermark is

```
    Input: System Parameters ($a = 2.8$, $b = 0.2$, $c = 1.4$, $d = 1$, $e = 10$, $f = 2$), Initial condition ($x(0) = 0$, $y(0) = 0$, $z(0) = 0$)
    Output: Chaos-Based Random Numbers (CBRNG)
(1) Start
(2) Determination of the appropriate value of $\Delta h$ (0.05)
(3) while minimum 1Mbit data do
        Solving the chaotic system using the RK-4 algorithm
        Obtaining time series
        Convert float to binary
        Select "$s = 16$" bit LSB
    end while
(4) Apply randomness tests
(5) if test results = = pass then
        Ready-tested random numbers for engineering application
      else
        Test results = = false
        return Start
      end if
(6) Exit.
```

Algorithm 1: Chaos-Based Random Number Generator (CBRNG).

Table 1: RNG NIST-800-22 tests with a 3D chaotic system without equilibrium points.

Statistical tests	P value (x)	Result
Frequency (monobit) test	0.6326	Successful
Block-frequency test	0.4965	Successful
Cumulative-sums test	0.6356	Successful
Runs test	0.0684	Successful
Longest-run test	0.8196	Successful
Binary matrix rank test	0.1178	Successful
Discrete Fourier transform test	0.7342	Successful
Nonoverlapping templates test	0.0053	Successful
Overlapping templates test	0.2708	Successful
Maurer's universal statistical test	0.2039	Successful
Approximate entropy test	0.6650	Successful
Random excursions test	0.4787	Successful
Random excursions variant test	0.6745	Successful
Serial test 1	0.5894	Successful
Serial test 2	0.6463	Successful
Linear complexity test	0.3089	Successful

placed on the cover image, pixel by pixel, to its previous positions with CBRNG. In this way, it is aimed to discover watermarking difficult.

According to Figure 7, random numbers were generated (CBRNG) with the proposed chaotic system according to the size (256 × 256) of the B matrix to be obtained. Then, the N-dimensional RNG array was obtained. In Figure 7, the B matrix is created by selecting the green pixel values of the CBRNG array of the cover image. With the watermark hidden in the B matrix with the proposed method, the 256 × 256 matrix B with the watermark shown in red in Figure 7 is obtained. As a result of the watermarking, the watermarked matrix is repositioned to the CBRNG array pixels marked in red. Since the watermarking process is performed on random numbers indicated by the CBRNG series, the chaotic system that makes up the CBRNG number system must be known to obtain the secret watermark.

The algorithm's pseudocode for generating the B matrix in the proposed chaos-based RNG watermarking method is given in Algorithm 2.

According to Algorithm 2, the width (Width1) and height (Height1) values of matrix B are taken as input. Then, the cover image (img1) to be processed is selected, and the width (Width) and height (Height) values are read. By selecting the RNG file, the CBRNG sequence is divided into two: CBRNG X and Y. The values in the CBRNG array are checked and parsed as repetitive values. This is to avoid using the same location twice, thanks to unique values. The elements of the CBRNG X array are normalized with the width value and the elements of the CBRNG Y array with the height value, so the array number values are adjusted according to the width and height limit of the original image. An empty array is created according to the desired Width1 and Height1 values for the B matrix to be obtained. Two nested loops are created. It starts from the first row and first column of matrix B. All the image pixels are processed until the outer loop to the value of Height1 in the first iteration and the value of Width1 in the first iteration of the inner loop. In Algorithm 2, the outer loop variable i shows the rows in the cover image; if the inner loop variable j shows the column row, CBRNG Y shows the rows, and CBRNG X shows the random number generator values for the columns. In each step of the loop, the pixel of the cover image is taken at the position determined by the CBRNG sequence and placed in the next pixel of the B matrix. This process continues until all pixels of matrix B have been generated.

4.2. Obtaining Cover/Watermarked Cover Image from Selected Blocks Matrix. In the proposed chaos-based CBRNG watermarking method, the flow diagram of the algorithm for placing the watermarked matrix B back to its previous positions in the cover image is given in Algorithm 3. By selecting the watermarked matrix B to be obtained according to Algorithm 3, the width (Width1) and height (Height1)

Table 2: ENT test results of random numbers obtained from x output.

Test name	Average	Ideal results	Result
Arithmetic mean	127.4068	127,5	Successful
Entropy	7.9985	8	Successful
Correlation	0.0012006	0	Successful
Chi-square	252.137	Between 10% and 90%	Successful
Monte Carlo	3.1331 (error = 0.0027013)	Pi number	Successful

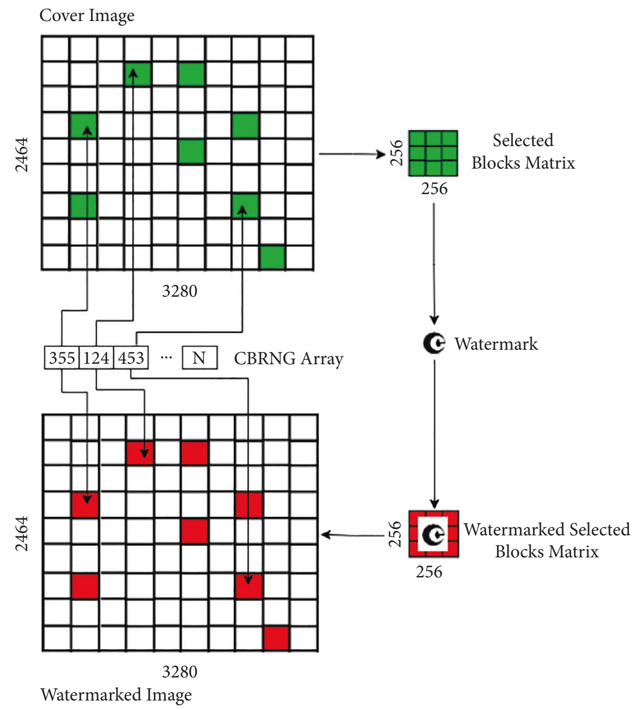


Figure 7: Working principle of the proposed chaos-based RNG watermarking method.

values are read. Then, by selecting the cover image (img1) to be processed, the width (Width) and height (Height) values are obtained. By selecting the CBRNG file, the CBRNG sequence is divided into two CBRNG X, and Y. Duplicate values are parsed by checking the values in the CBRNG array. This avoids using the same location twice, thanks to unique values. The elements of the CBRNG X array are normalized with the width value, and the elements of the CBRNG Y array with the height value so that the array number values are set according to the width and height limit of the original image. Two nested loops are created. It starts from the first row and first column of matrix B. All the image pixels are processed until the outer loop to the value of Height1 in the 1st iteration and the value of Width1 in the 1st iteration of the inner loop. In Algorithm 3, the outer loop variable i represents the rows in the original image; if the inner loop variable j is the column row, CBRNG Y represents the rows, and CBRNG X represents the random number generator values for the columns. At each step of the loop, the pixel of matrix B in the j column position of the i row is taken and placed in the cover image pixel at the position determined by the CBRNG array. This process continues until all the indices of the watermarked matrix B have been placed back. Thus, a watermarked image is obtained by using CBRNG from matrix B. This process is also used in the watermarking and watermark removal algorithm.

4.3. DWT and SVD Methods. Discrete wavelet transform is one of the most basic methods that transform digital images from the spatial domain to the frequency domain. DWT is a feature extraction technique that allows the processing of images at different resolutions. It is especially preferred in watermarking research because it is resistant to attacks applied to the image [68]. In this study, R-level DWT, which considers the size of the selected blocks matrix and the watermark size, is used. Here, R is determined according to the result of the expression $\log_2(M/N)$. For example, if $M = 512$ and $N = 128$, $R = 2$. Therefore, 2-level DWT is applied. After the DWT process, LL for low frequency, HL for horizontal mid-frequency, LH for vertical mid-frequency, and HH for high frequency are obtained. Performing the DWT process R times on these subbands obtained from the previous DWT operation is called R-LEVEL DWT. For example, Figure 8 shows the subbands obtained due to 1-level DWT and 2-level DWT.

Singular value decomposition (SVD), mainly used for dimension reduction in signal processing studies, is preferred in watermarking because it is more resistant to attacks. Assuming $A \in \mathbb{R}^{m\times n}$ and $m > n$, A is factored by the SVD operation as shown in the following equation:

$$A = U\Sigma V^T. \tag{6}$$

The matrices U and V here are orthogonal and satisfy the conditions $UU^T = U^TU = I$ and $VV^T = V^TV = I$, respectively. The Σ is a diagonal matrix, and it satisfies the condition $\sigma_1 > \sigma_2 >, \ldots, > \sigma_m$, the diagonal elements being $\sigma_1, \sigma_2, \ldots, \sigma_m$, respectively.

4.4. Proposed Watermarking Scheme. In this article, numbers produced by a chaos-based number generator and watermarking techniques were combined to protect medical confidentiality, and digital watermarking was made on medical images. The study considers a new binary watermarking scheme that includes encryption to improve medical images' tenure, protection, and robustness. The security feature of the proposed watermarking technique is enhanced by chaos-based and uniquely number generation. The watermarked primary image is encrypted using the chaos-based encryption technique. It is then placed in the image and transmitted. The chaotic encryption scheme

```
     Input: Cover/Watermarked Image
     Output: Selected Block Matrix (B)
 (1) Start
 (2) Read Cover Image (img1)
 (3) Get Width and Height from img1
 (4) Select CBRNG file
 (5) Divide CBRNG numbers by CBRNG $X$ and CBRNG Y
 (6) Normalize the values in the CBRNG $X$ array by modulo with Width
 (7) Normalize the values in the CBRNG Y array by modulo with Height
 (8) Discard repetitive values in CBRNG $X$ and Y
 (9) Get Width1 and Height1 from B
(10) Create an array of size B
(11) for $i = 1$: Height1: 1
         for $j = 1$: Width1: 1
         $B(i, j)$ = img1(CBRNG Y($i$), CBRNG X($j$))
       end for
(12) Return $B$
(13) End
```

Algorithm 2: Generating the Selected Blocks Matrix.

```
     Input: Cover Image, $B^*$
     Output: Watermarked Image ($C^*$)
 (1) Start
 (2) Read Cover Image (img1)
 (3) Get Width and Height from img1
 (4) Select CBRNG file
 (5) Divide CBRNG numbers by CBRNG $X$ and CBRNG Y
 (6) Normalize the values in the CBRNG $X$ array by modulo with Width
 (7) Normalize the values in the CBRNG Y array by modulo with Height
 (8) Discard repetitive values in CBRNG $X$ and Y
 (9) Get array $B^*$
(10) Get Width1 and Height1 from $B^*$
(11) for $i = 1$: Height1: 1
         for $j = 1$: Width1: 1
         img1(CBRNG Y($i$), CBRNG X($j$)) = $B^*$ (i,j)
       end for
(12) Create $C^*$ from img1 array
(13) Return $C^*$
(14) End
```

Algorithm 3: Generating the Watermarked Image.

provides a large key space and high key precision, and the password can resist brute force attacks and statistical analyses. The proposed method is secure against third-party attacks and can meet the need for image encryption. A reliable watermark decryption scheme and an extraction scheme for both the primary and secondary watermark are established to remove the watermark. In the proposed method, the watermark is hidden in the image created by selecting random pixels with the numbers produced by RNG from the original image with medical content. The 8 bit images containing human blood and cancer cell samples were used. In the method, first, the watermark is hidden in the image created from the pixels selected with RNG from the original image. Then, the watermarked image is placed on the original image with RNG, pixel by pixel, to its previous positions. In this way, the method makes watermark detection difficult and makes it difficult to discover the watermark. The watermarked image recreated at the end of the method is not distinguishable from the original image. The watermark can be removed lossless from the watermarked image. The RNG sequence created through the chaotic system is needed for the watermark extraction process. By operating the chaotic system with the same initial conditions at the receiving end, the same RNG sequence can be produced, or a standard RNG sequence can be used. RNG sequence can be considered the proposed method's chaotic encryption algorithm. Different encryptions can be made by changing the RNG sequence. This

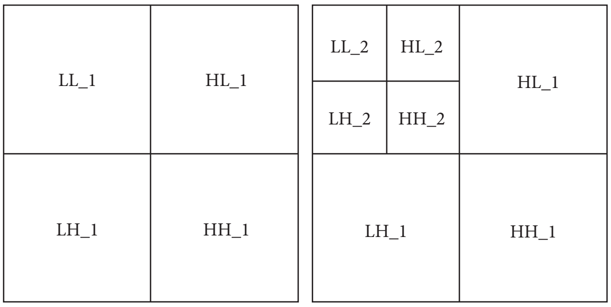


Figure 8: 1-level DWT and 2-level DWT.

increases the system's security and prevents malicious people from destroying the watermark.

In the next section, watermarking embedding and watermarking extraction algorithms are explained. In this algorithm, the cover image, selected block obtained with chaos-based random numbers, and the watermark are represented by $C \in \mathbb{R}^{x\times y}$, $B \in \mathbb{R}^{m\times m}$, and $W \in \mathbb{R}^{n\times n}$, respectively. After the watermarking embedding, $C^* \in \mathbb{R}^{x\times y}$ and $B^* \in \mathbb{R}^{m\times m}$ are obtained. After the watermarking extraction, $W^* \in \mathbb{R}^{n\times n}$ is obtained. Here, the condition $\forall x \forall y\,(x \geq m \geq n \wedge y \geq m \geq n)$ is met.

4.4.1. Watermarking Embedding Algorithm. First, B is obtained from the cover image (C) using CBRNG. In the second step, R-level DWT is applied to matrix B. The SVD is applied to the Rth LL (LL_R) obtained with the R-level DWT. U_B, Σ_B and V_B^T are obtained from this process. Also, singular value decomposition is applied to the W matrix and U_W, Σ_W and V_W^T matrices are obtained. Σ_B^* is obtained by taking into account the singular values (Σ_B and Σ_W) and the scaling factor (α) in

$$\Sigma_B^* = \Sigma_B + \alpha\Sigma_W. \tag{7}$$

In (8), using Σ_B^*, U_B, and V_B^T, LL_R^* is obtained.

$$LL_R^* = U_B \Sigma_B^* V_B^T. \tag{8}$$

With LL_R^*, the reverse of the R-level DWT process is applied and B^* is obtained. Then, using B^* and CBRNG, the pixels in C are updated and C^* is obtained. The watermarking embedding process is explained step by step in Algorithm 4. Figure 9 shows the proposed watermarking embedding scheme.

4.4.2. Watermarking Extraction Algorithm. In this algorithm, Watermarked hologram Image (C^*) and the CBRNG used in the watermarking embedding algorithm are taken as inputs. As the output, the extracted watermark W^* is obtained. As in the watermarking embedding algorithm, the watermarked selected block (B^*) is obtained from the C^* image using the same CBRNG.

Then, R-level DWT is applied to the B^* matrix and LL_W^*, HL_W^*, LH_W^* is obtained. SVD is applied to the LL_W^* and U_E, Σ_E and V_E^T matrices are obtained. Then, the singular values of the watermark are extracted using the Σ_B obtained during watermarking embedding process with

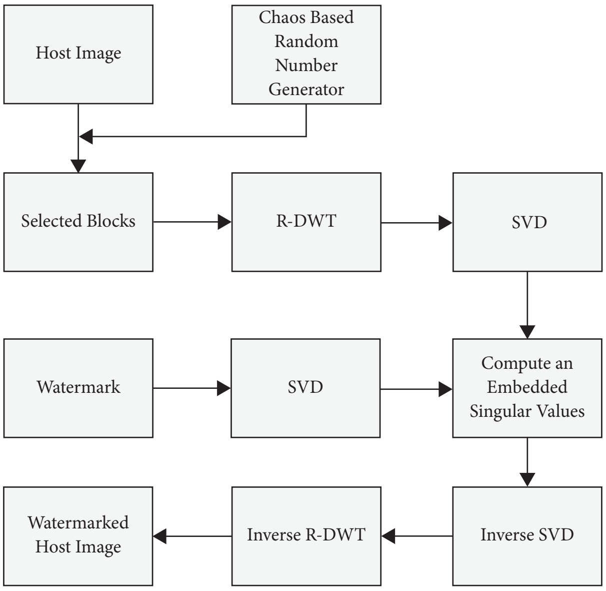


Figure 9: Proposed watermarking embedding scheme.

$$\Sigma_W^* = \frac{(\Sigma_E - \Sigma_B)}{\alpha}. \tag{9}$$

Using the Σ_W^* and U_W, and V_W^T, the extracted watermark W^* is obtained by equation (10). The watermarking extraction process is explained step by step in Algorithm 5. Figure 10 shows the proposed watermarking extraction scheme.

$$W^* = U_W \Sigma_W^* V_W^T. \tag{10}$$

5. Experimental Results and Safety Analysis

In this section, performance tests were conducted to analyze the invisibility and the robustness of the proposed technique in this study. The human blood and cancer cell line images shown in Figure 11 are used as the cover image. The textual data in Figure 12(a) for blood images and Figure 12(b) for cancer images were used as watermarks. The QR codes as the visual representation of the texts given in Figures 12(a) and 12(b) are shown in Figure 13, respectively. All of the experiments were carried out on a Workstation with an Intel dual-core 2.7 GHz CPU with 32 GB of RAM, using the MATLAB R2018b version.

The proposed model's time complexity is relatively low, considering that the watermark size is much smaller than the cover image size. The size of the watermark image is $a \times b$. Here the condition $a > b$ and $a < \min(m, n)$ is satisfied. Accordingly, the time complexity of the proposed method is ab^2. Here, a and b values are smaller than the dimensions of the cover image (m and n). The a and b values are very small relative to the dimensions of the cover image (m and n). Therefore, the time complexity of the proposed algorithm is not dependent on the size of the cover image.

```
Input: Cover Image $(C)$, Watermark Image $(W)$, scaling factor $(\alpha)$
Output: Watermarked Hologram Image $(H^*)$
Start
$B$ = Generating the Selected Blocks Matrix (C)
$[LL_R, HL_R, LH_R$ ve $HH_R] = R$_Level_DWT(B)
SVD is applied to the $LL_R$ and $U_B, \Sigma_B$ and $V_B^T$ are obtained.
SVD is applied to the $W$ and $U_W, \Sigma_W$ and $V_W^T$ are obtained.
$\Sigma_B^* = \Sigma_B + \alpha\Sigma_W$
$LL_R^* = U_B \Sigma_B^* V_B^T$
$B^*$ = InverseRlevelDWT$(LL_R^*, HL_R, LH_R HH_R)$
$C^*$ =Generating the Watermarked Image $(C, B^*)$
return $C^*$.
End.
```

Algorithm 4: Watermarking Embedding Algorithm.

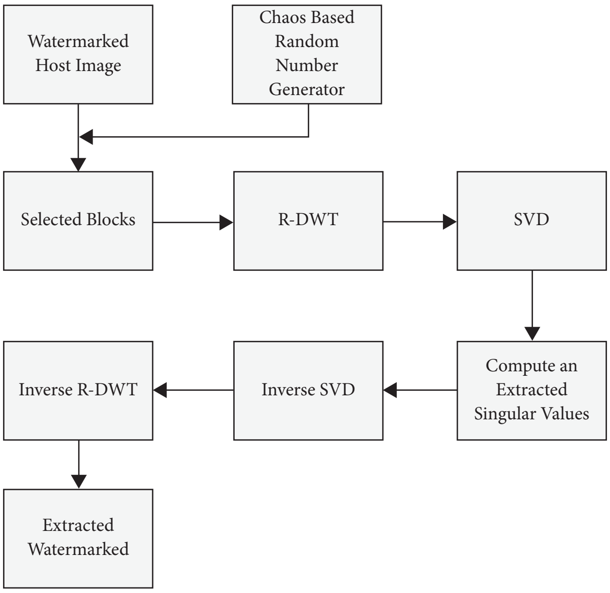


Figure 10: Proposed watermarking extraction scheme.

```
Input: Watermarked Cover Image $(C^*)$
Output: Extracted watermark $(W^*)$
Start
$B^*$ =Generating the Selected Blocks Matrix $(C^*)$
$[LL_W^*, HL_W^*, LH_W^*, HH_W^*] = R$_Level_DWT $(B^*)$
SVD is applied to the $LL_W^*$ and $U_E, \Sigma_E$ ve $V_E^T$ are obtained.
$\Sigma_W^* = (\Sigma_E - \Sigma_B)/\alpha$
$W^* = U_W \Sigma_W^* V_W^T$
return $W^*$.
End.
```

Algorithm 5: Watermarking Extraction Algorithm.

The chaos-based random numbers were used to cope with the false positive problem encountered in the SVD technique used in the study. Tests were carried out to see if the proposed model was resistant to false positive problems. Table 3 provides the images and robustness results of the extracted watermark in cases where the chaotic keys are entered correctly or incorrectly. The results were obtained using the blood cell cover image and a 256 × 256 watermark. It is understood from the table that the watermark was not extracted correctly in all rows except the first row, where the

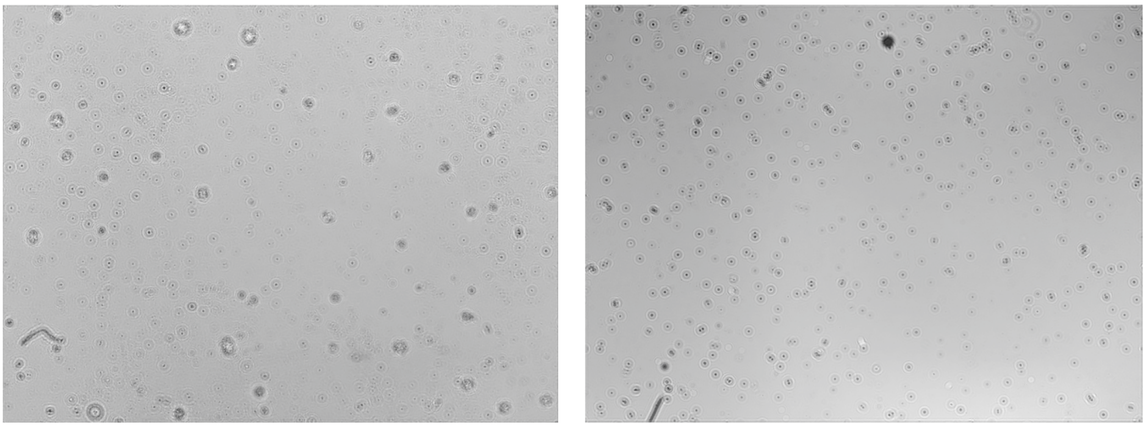
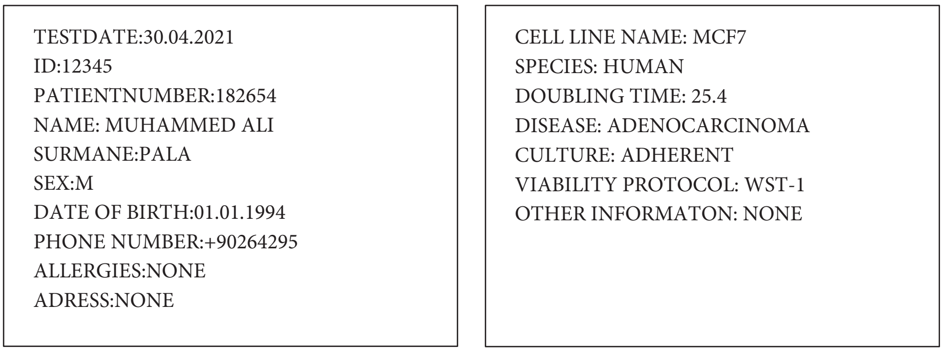

(a)
(b)

Figure 11: Sample blood and cancer cell images (256 × 256).


TESTDATE:30.04.2021
ID:12345
PATIENTNUMBER:182654
NAME: MUHAMMED ALI
SURMANE:PALA
SEX:M
DATE OF BIRTH:01.01.1994
PHONE NUMBER:+90264295
ALLERGIES:NONE
ADRESS:NONE

(a)

CELL LINE NAME: MCF7
SPECIES: HUMAN
DOUBLING TIME: 25.4
DISEASE: ADENOCARCINOMA
CULTURE: ADHERENT
VIABILITY PROTOCOL: WST-1
OTHER INFORMATON: NONE

(b)

Figure 12: Watermark texts (a) for cancer cell image and (b) blood image.

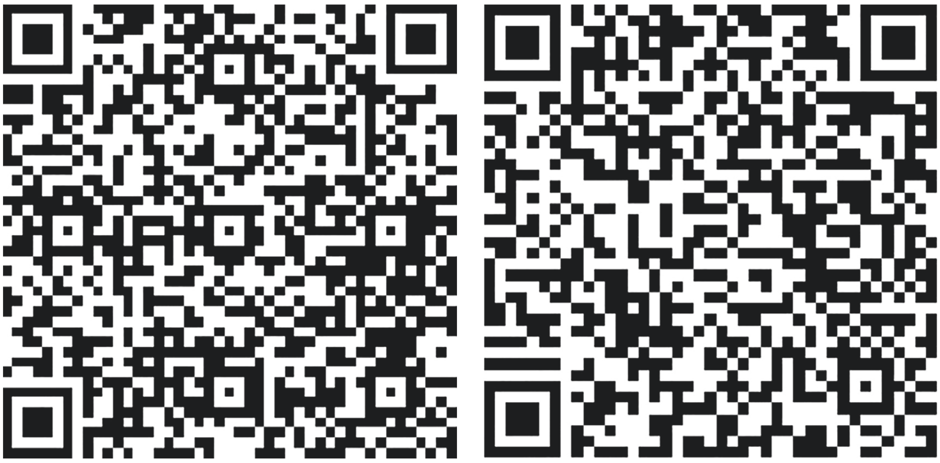
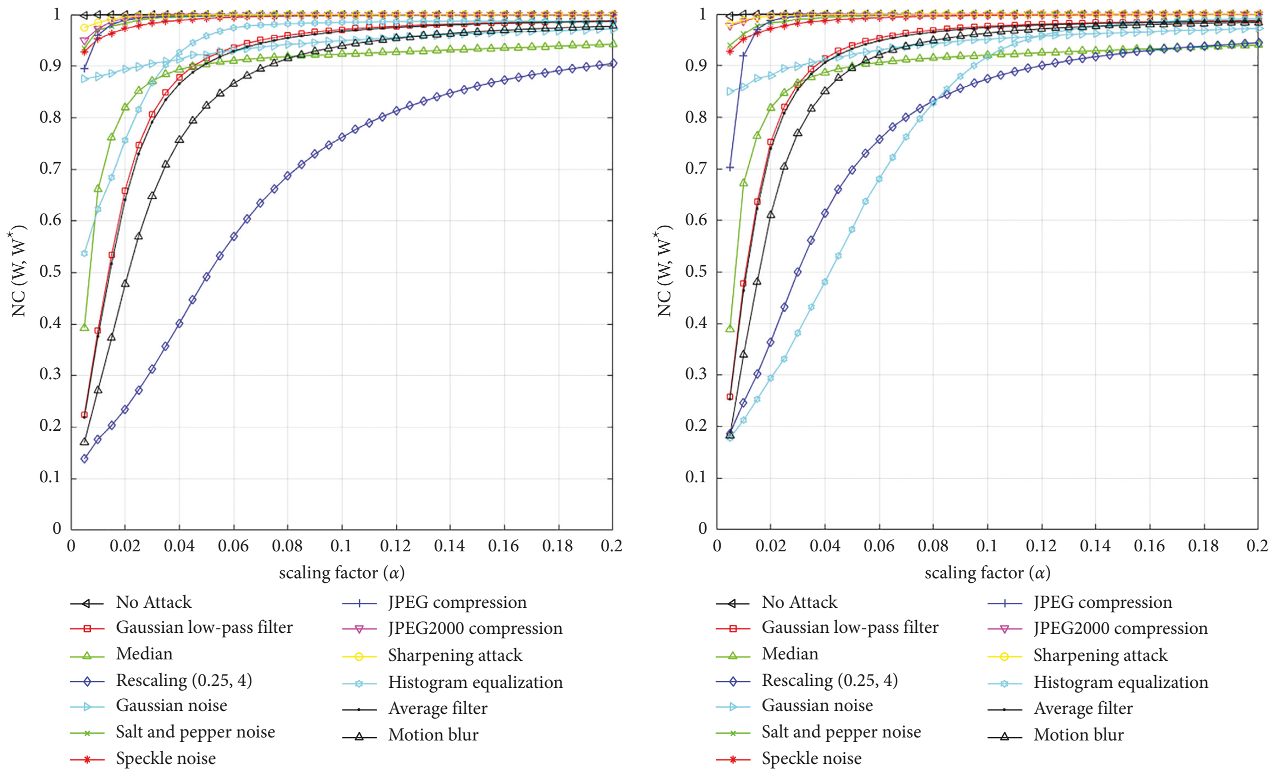

(a)
(b)

Figure 13: Watermark QR codes (256 × 256). (a) Watermark QR code for blood images and (b) cancer cell line images.

Table 3: FPP analysis result.

System parameters	Initial condition	NC
$a = 2.8,\ b = 0.2,\ c = 1.4,\ d = 1,\ e = 10,\ f = 2$	$x0 = 0,\ y0 = 0,\ z0 = 0$	1
$a = 1.8,\ b = 0.2,\ c = 1.4,\ d = 1,\ e = 10,\ f = 2$	$x1 = 1,\ y0 = 0,\ z0 = 0$	0.5912
$a = 1.8,\ b = 0.4,\ c = 1.4,\ d = 1,\ e = 10,\ f = 2$	$x1 = 1,\ y0 = 1,\ z0 = 0$	0.5221
$a = 1.8,\ b = 0.4,\ c = 1.0,\ d = 1,\ e = 10,\ f = 2$	$x1 = 1,\ y0 = 1,\ z0 = 1$	0.4766
$a = 1.8,\ b = 0.4,\ c = 1.0,\ d = 2,\ e = 10,\ f = 2$	$x1 = 1,\ y0 = 1,\ z0 = 1$	0.4643
$a = 1.8,\ b = 0.4,\ c = 1.0,\ d = 2,\ e = 5,\ f = 2$	$x1 = 1,\ y0 = 1,\ z0 = 1$	0.4539
$a = 1.8,\ b = 0.4,\ c = 1.0,\ d = 2,\ e = 5,\ f = 1$	$x1 = 1,\ y0 = 1,\ z0 = 1$	0.4304



(a)

(b)

Figure 14: NC results of tests under different attacks according to scaling factor change. (a) Human blood. (b) Cancer cell line.

correct keys were entered. Accordingly, it is impossible to extract the watermark for someone who does not know the keys of the random number generator and the chaos function used in the proposed model.

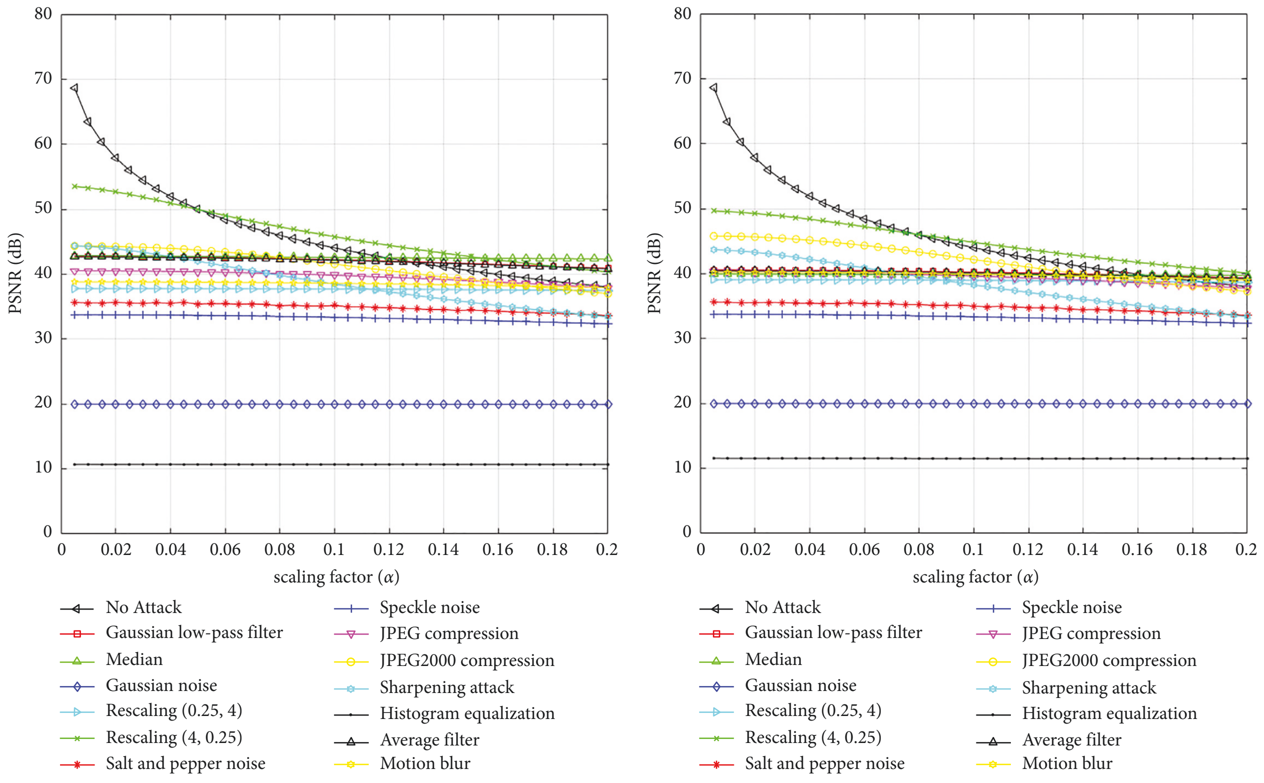
In order to obtain the best performance in the watermarking algorithm, the optimal scaling factor must be found. Normalized correlation (NC) is used for watermark robustness for performance analysis. In contrast, peak signal-to-noise ratio (PSNR) and structural similarity index measure (SSIM) metrics measure watermark imperceptibility. The calculation of the NC is shown in the following equation.

$$\mathrm{NC}\left(W, W^{*}\right) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} W_{i,j}W_{i,j}^{*}}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} W_{i,j}^{2}}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} W_{i,j}^{*2}}}. \tag{11}$$

Equations for calculating MSR, PSNR, and SSIM metrics are

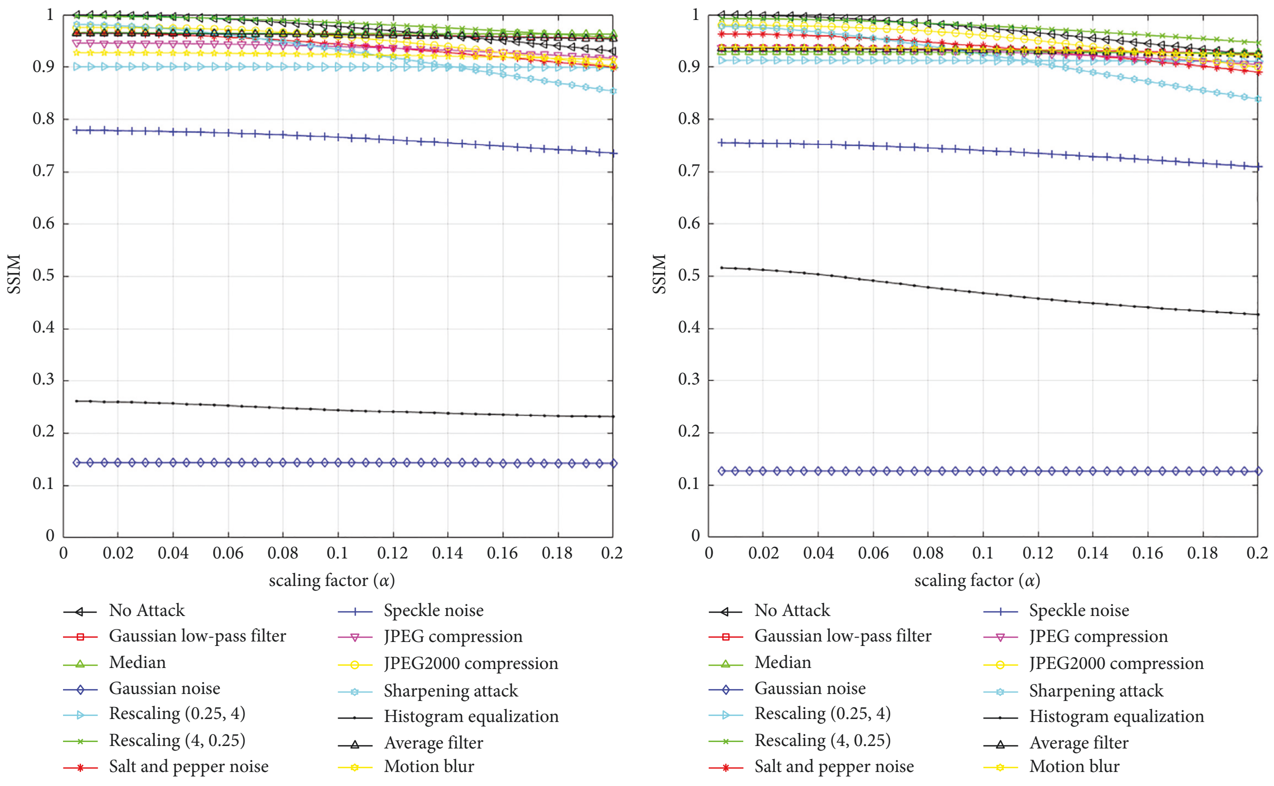
$$\mathrm{MSE}\left(C, C^{*}\right) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}\left(C_{i,j} - C_{i,j}^{*}\right)}{M^{2}}, \tag{12}$$

$$\mathrm{PSNR}\left(C, C^{*}\right) = 10\ \log_{10}\frac{C_{\max}^{2}}{MSE\left(C, C^{*}\right)}, \tag{13}$$



(a) (b)

FIGURE 15: PSNR results of tests under different attacks according to scaling factor change. (a) Human blood. (b) Cancer cell line.



(a) (b)

FIGURE 16: SSIM results of tests under different attacks according to scaling factor change. (a) Human blood. (b) Cancer cell line.

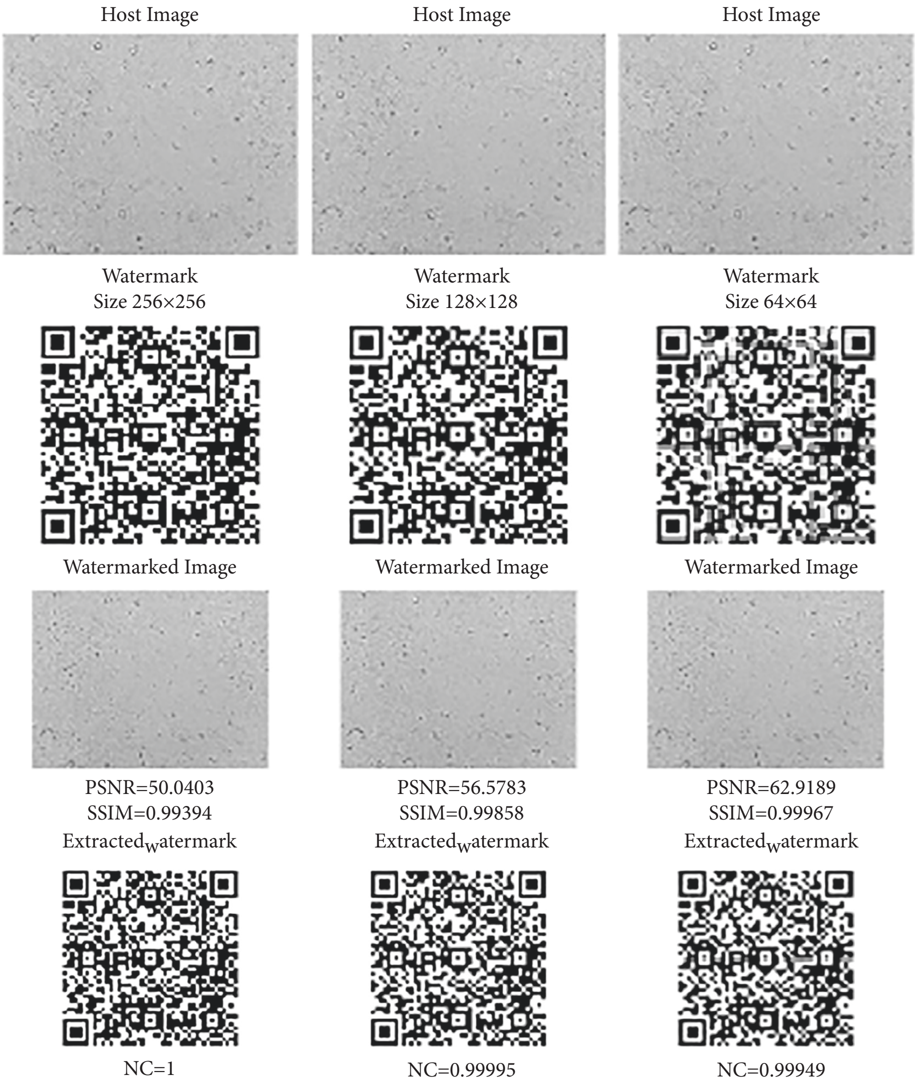


Figure 17: Invisibility performance of blood image.

$$\mathrm{SSIM}\left(C, C^{*}\right)=\frac{2\mu_c\mu_{c^*}+v_1}{\mu_C^2+\mu_{C^*}^2+v_1}\cdot\frac{\alpha_{CC^*}+v_2}{\alpha_C^2+\alpha_{C^*}^2+v_2}. \tag{14}$$

The μ_c and μ_{c^*} in the equations are the mean of C and C^*, respectively. α_C^2 and $\alpha_{C^*}^2$ are the variances of C and C^*. v_1 and v_2 are two variables used to balance the partition with a weak denominator. Finally, α_{CC^*} is the covariance of C and C^*.

For the robustness and invisibility analysis of the watermark, three forms of watermarks (64 × 64, 128 × 128, and 256 × 256) were used. The best scaling factors for all three forms and each cover image were determined by considering the changes in NC, PSNR, and SSIM metrics. For the robustness analysis, various attacks were applied to the watermarked image, and the watermark's invisibility was examined. In addition, robustness analyses were performed on the watermark extracted from the watermarked image. The applied attacks are basically noise (Gaussian, salt and peppers, and speckle noises), filter (median, Gaussian lowpass, and average), compression (JPEG with quality factor (QF) 50 and JPEG2000 with compression ratio (CR) 12), rescaling (0.25, 4), histogram equalization (HE), sharpening (threshold = 0.8), and motion blur (with Theta = 4, Len = 7) attacks.

It is necessary to analyze the durability of watermark and the cover image's imperceptibility to determine the optimum scaling factor. For this, both NC values, as well as PSNR and SSIM metrics, were examined. Accordingly, cases where all three metrics are good can be selected as the scaling factor. In order to determine the optimum scaling factor, NC change under various attacks is shown in Figure 14 for blood and cancer cell line images, respectively. PSNR and SSIM results are also shown in Figures 15 and 16, respectively. When the changes are examined, the NC value increases as the alpha increases, while the PSNR and SSIM results decrease. In cases where noisy attacks such as Gaussian noise, speckle noise, salt and pepper noise, compression, and sharpening attacks are applied, the results give good results even at smaller alpha values. For example, relevant results

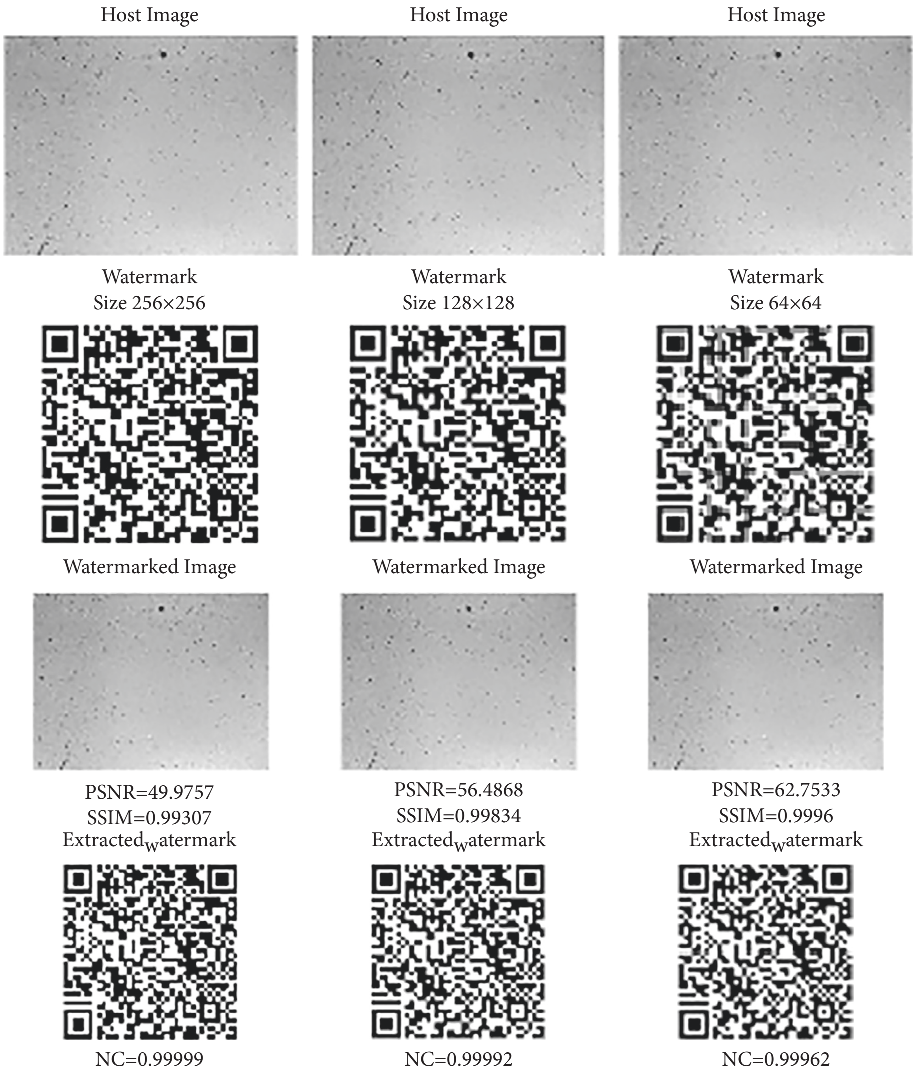


Figure 18: Invisibility performance of cancer cell line image.

were obtained when these attacks were applied even when $\alpha = 0.01$.

Another issue to be measured in watermarking studies is invisibility. The fact that people cannot notice the watermarked information is essential for the security of the data. In this case, it is aimed that the watermarked image obtained after watermarking does not look much different from the original. For this reason, invisibility measurement is essential in order not to understand the watermark in the watermarked image. Figures 17 and 18 show the invisibility and robustness results obtained for exemplary blood and cancer cell line images, respectively. The watermark texts were transformed into QR codes in 256×256, 128×128, and 64×64 sizes. Here, the performance results after these three different watermarking are listed.

When Figures 17 and18 are examined, 100% successful access to the texts is achieved from the QR codes obtained. The literature states that acceptable invisibility is when the measured values for invisibility are PSNR>0.37 dB and

Table 4: The robustness performance of the watermarked blood image obtained using different-sized watermarks.

Attack	Watermark size		
	256×256	128×128	64×64
No attack	1	0.99999	0.99994
Gaussian low-pass filter	0.98809	0.96782	0.95473
Median	0.94269	0.92397	0.94444
Gaussian noise	0.97201	0.97087	0.98694
Rescaling (0.25, 4)	0.90461	0.88459	0.86823
Rescaling (4, 0.25)	0.99985	0.99956	0.99923
Salt and pepper noise	0.99971	0.99973	0.99961
Speckle noise	0.9994	0.99933	0.99948
JPEG compression	0.99875	0.99353	0.97793
JPEG2000 compression	0.99959	0.99915	0.99391
Sharpening attack	0.99995	0.98755	0.98443
Histogram equalization	0.98631	0.97033	0.96303
Average filter	0.98684	0.96459	0.94941
Motion blur	0.9775	0.95125	0.93015

Table 5: The robustness performance of the watermarked cancer cell line image obtained using different-sized watermarks.

Attack	Watermark size		
	256 × 256	128 × 128	64 × 64
No attack	0.99988	0.99999	0.99996
Gaussian low-pass filter	0.98733	0.97427	0.96717
Median	0.93992	0.93212	0.94764
Gaussian noise	0.97206	0.96799	0.98251
Rescaling (0.25.4)	0.94459	0.89711	0.87132
Rescaling (4.0.25)	0.99944	0.99947	0.99914
Salt and pepper noise	0.99953	0.99954	0.99955
Speckle noise	0.99899	0.99925	0.99944
JPEG compression	0.99919	0.99268	0.97928
JPEG2000 compression	0.99943	0.99915	0.99740
Sharpening attack	0.9997	0.98721	0.98400
Histogram equalization	0.9911	0.84563	0.83418
Average filter	0.98625	0.97174	0.96350
Motion blur	0.98371	0.9686	0.95394

SSIM>0.93. When all the images here are examined, it is observed that a value far above these limits is obtained. In addition, if the QR code images are taken into account, it has been observed that the NC results of the recalled watermarks are very close to 1.

Tables 4 and 5 provide the normalized correlation (robustness) of images against various attacks. Here, 256 × 256, 128 × 128, and 64 × 64 sized QR codes were watermarked separately, and the results were listed after these three different watermarks.

When Tables 4 and 5 are examined, it is seen that a robust watermarking process is performed for the sample blood and the sample cancer cells in the no attack condition. As the watermark size decreased, the performance decreased slightly, but outstanding results were still obtained.

There is almost no loss in the watermark after the applied noise (Gaussian, salt and peppers, and speckle noises) attacks. Similarly, outstanding performances were obtained in each Gaussian low-pass filter, rescaling (4, 0.25), JPEG compression, JPEG2000 compression, and sharpening attacks. It has been observed that the median and average filter attacks, rescaling (0.25.4), histogram equalization, and motion blur attacks are good enough but not as good as the above attacks. Outstanding results were obtained in all attacks, mainly when a 256 × 256 watermark was applied. Although the results obtained for Histogram equalization and Rescaling (0.25.4) attacks were sufficient when 128 × 128 and 64 × 64 size watermarks were applied, the robustness decreased more than the others. Lossless results were obtained in almost all of the proposed watermark methods against all attacks except these attacks. After the QR code of all watermarks is converted back to the text, completely lossless watermark texts are obtained.

6. Conclusion

Watermarking has excellent potential to provide valuable solutions for medical applications such as identity theft, data security, health data management, and storage. This study developed a new method using chaos-based discrete wavelet transform (DWT) and singular value decomposition (SVD) for watermarking with high imperceptibility and robustness. In order to obtain a high-resolution biomedical image, a low-cost, large field of view and easy-to-integrate LED-based DIHM setup was designed. The resolution capability of the imaging system is demonstrated with the standard USAF 1951 resolution target. The captured diffraction patterns of medical samples were reconstructed using the angular spectrum method. Images of human blood and cancer cell lines, which are widely used in the laboratory environment, were obtained. For the security feature of the proposed watermarking technique, chaos-based random number generators are used. Specifically, chaos-based random number generators were used to eliminate the false positive problem, which is the disadvantage of the SVD method. The chaotic system without equilibrium points is preferred for the chaos-based random number generator. The suitability of the selected chaotic system for use in studies such as encryption, data hiding, and watermarking has been proven by dynamic analysis. Random numbers are generated with CBRNG as the same random numbers are needed when the system is rerun for the watermarking application. NIST-800-22 and ENT statistical tests with the highest standards at the international level were used to measure the randomness performance of the numbers produced. For the watermarking process, a new method using chaos-based discrete wavelet transform (DWT) and singular value decomposition (SVD) has been developed and applied to high-resolution data in order to eliminate the problem of encrypted data being directly targeted by third-party attacks. The performance of the proposed new watermarking method has been demonstrated by various robustness and invisibility tests. Robustness and invisibility results show the watermarked host images have good visual quality, PSNRs, and SSIMs. Experimental results showed that the proposed scheme reached an average PSNR value of 564588 dB and an SSIM value of 0.9972 against several geometric and destructive attacks. Furthermore, the watermarks can be clearly extracted from the watermarked host image, and even for the watermarks with different sizes, the proposed image watermarking method achieved good invisibility and robustness. To the best of our knowledge, the proposed method has been applied for the first time in DIHM systems, along with producing solutions to the problems in the watermarking process. The proposed method can be applied to medical images obtained in both clinical and laboratory conditions and has the potential to be applied to many different high-resolution data. We can apply our proposed method to color images and many other areas in our future work. It is also possible to construct a blind and more secure watermarking system using some cutting-edge techniques like blockchain, deep learning, or machine learning, and better error-correcting code.

Data Availability

The datasets generated during and/or analyzed during the current study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Sakarya University of Applied Science Scientific Research Projects Coordination Unit (SUBU BAPK, Project Number: 2020-01-01-011). The author, Muhammed Ali PALA, is grateful to The Scientific and Technological Research Council of Turkey for granting a scholarship (TUBITAK, 2211-C) for his Ph.D. studies.

References

[1] K. Y. Ngiam and I. W. Khor, "Big data and machine learning algorithms for health-care delivery," *The Lancet Oncology*, vol. 20, no. 5, pp. 262–273, 2019.

[2] G. Manogaran, C. Thota, D. Lopez, V. Vijayakumar, K. M. Abbas, and R. Sundarsekar, *Big Data Knowledge System in Healthcare*, pp. 133–157, Springer, Cham, Switzerland, 2017.

[3] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "An efficient medical image watermarking scheme based on FDCuT–DCT," *Engineering Science and Technology, an International Journal*, vol. 20, no. 4, pp. 1366–1379, 2017.

[4] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking techniques used in medical images: a survey," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 714–729, 2014.

[5] S. Sharma, H. Sharma, J. B. Sharma, and R. C. Poonia, "A secure and robust color image watermarking using nature-inspired intelligence," *Neural Computing & Applications*, pp. 1–19, Jan. 2021.

[6] R. Dhanalakshmi and K. Thaiyalnayaki, "Dual watermarking scheme with encryption," *International Journal of Computer Science and Information Security*, vol. 7, no. 1, pp. 248–253, 2010.

[7] S. Sharma, H. Sharma, and J. B. Sharma, "Artificial intelligence based watermarking in hybrid DDS domain for security of colour images," *International Journal of Intelligent Engineering Informatics*, vol. 8, no. 4, p. 331, 2020.

[8] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Robust and imperceptible dual watermarking for telemedicine applications," *Wireless Personal Communications*, vol. 80, no. 4, pp. 1415–1433, 2015.

[9] S. A. K. Mostafa, N. El-sheimy, A. S. Tolba, F. M. Abdelkader, and H. M. Elhindy, "Wavelet packets-based blind watermarking for medical image management," *The Open Biomedical Engineering Journal*, vol. 4, no. 1, pp. 93–98, 2010.

[10] S. Sharma, H. Sharma, and J. B. Sharma, "An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization," *Applied Soft Computing*, vol. 84, Article ID 105696, 2019.

[11] R. Pandey, A. K. Singh, B. Kumar, and A. Mohan, "Iris based secure NROI multiple eye image watermarking for teleophthalmology," *Multimedia Tools and Applications*, vol. 75, no. 22, Article ID 14381, 2016.

[12] H. Nyeem, W. Boles, and C. Boyd, "A review of medical image watermarking requirements for teleradiology," *Journal of Digital Imaging*, vol. 26, no. 2, pp. 326–343, 2013.

[13] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3669–3697, 2017.

[14] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8381–8401, 2016.

[15] K. A. Navas and M. Sasikumar, "Survey of medical image watermarking algorithms," in *Proceedings of the 4 th International conference: Sciences of Electronic, Technologies of Information and Telecommunications*, pp. 25–29, Tunisia, July 2007.

[16] M. AlShaikh, M. Alzaqebah, and S. Jawarneh, "Robust watermarking based on modified Pigeon algorithm in DCT domain," *Multimedia Tools and Applications*, pp. 1–21, 2022.

[17] L. Y. Hsu, H. T. Hu, and H. H. Chou, "A high-capacity QRD-based blind color image watermarking algorithm incorporated with AI technologies," *Expert Systems with Applications*, vol. 199, Article ID 117134, 2022.

[18] F. Ernawan, A. Aminuddin, D. Nincarean, M. F. A. Razak, and A. Firdaus, "Three layer authentications with a spiral block mapping to prove authenticity in medical images," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 4, pp. 211–223, 2022.

[19] D. Muigai, E. Mwangi, and E. T. Mharakurwa, "A prediction error nonlinear difference expansion reversible watermarking for integrity and authenticity of DICOM medical images," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 3, pp. 201–210, 2022.

[20] S. Huang and J. K. Wu, "Optical watermarking for printed document authentication," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 2, pp. 164–173, Jun. 2007.

[21] L. Xie and G. R. Arce, "Joint wavelet compression and authentication watermarking," *IEEE Int. Conf. Image Process.*vol. 2, pp. 427–431, 1998.

[22] P. Arena, A. Basile, L. Fortuna, M. E. Yalçin, and J. Vandewalle, "Watermarking for the authentication of video on CNN-UM," *Proceedings of the 2002 7th IEEE International Workshop on Cellular Neural Networks and Their Applications*, vol. 2002, Article ID 1035038, 83 pages, 2002.

[23] P. Sidiropoulos, N. Nikolaidis, and I. Pitas, "Invertible chaotic fragile watermarking for robust image authentication," *Chaos, Solitons & Fractals*, vol. 42, no. 5, pp. 2667–2674, 2009.

[24] W. H. Lin, S. J. Horng, T. W. Kao et al., "Image copyright protection with forward error correction," *Expert Systems with Applications*, vol. 36, no. 9, Article ID 11888, 2009.

[25] J. Zain and M. Clarke, *Security in Telemedicine: Issues in Watermarking Medical Images*, Brunel University, London, UK, 2005.

[26] M. M. Soliman, A. E. Hassanien, N. I. Ghali, and H. M. Onsi, "An adaptive watermarking approach for medical imaging using swarm intelligent," *Int. J. Smart Home*, vol. 6, no. 1, pp. 37–50, 2012.

[27] K. Pal, G. Ghosh, and M. Bhattacharya, "Biomedical image watermarking in wavelet domain for data integrity using bit majority algorithm and multiple copies of hidden information," *American Journal of Biomedical Engineering*, vol. 2, no. 2, pp. 29–37, 2012.

[28] N. A. Memon and S. A. M. Gilani, "NROI watermarking of medical images for content authentication," in *Proceedings of the 2008 IEEE International Multitopic Conference 2008 12th IEEE Int. Multitopic Conf. - Conf. Proc*, pp. 106–110, IEEE, Karachi, Pakistan, December 2008.

[29] C. C. Lai and C. C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value

decomposition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060–3063, 2010.

[30] A. Kannammal, K. Pavithra, and S. SubhaRani, "Double watermarking of dicom medical images using wavelet decomposition technique," *European Journal of Scientific Research*, vol. 70, no. 1, pp. 46–55, 2012.

[31] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communications*, vol. 152, pp. 72–80, Feb. 2020.

[32] P. Kadian, N. Arora, and S. M. Arora, "Performance evaluation of robust watermarking using DWT-SVD and RDWT-SVD," in *Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 987–991, IEEE, Noida, India, May 2019.

[33] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, "A lossless DWT-SVD domain watermarking for medical information security," *Multimedia Tools and Applications*, vol. 80, no. 16, Article ID 24823, 2021.

[34] E. McLeod and A. Ozcan, "Unconventional methods of imaging: computational microscopy and compact implementations," *Reports on Progress in Physics*, vol. 79, no. 7, Article ID 076001, 2016.

[35] W. Zhang, L. Cao, D. J. Brady et al., "Twin-image-Free holography: a compressive sensing approach," *Physical Review Letters*, vol. 121, no. 9, Article ID 093902, 2018.

[36] G. DIng, J. Wang, J. Zou et al., "A novel method based on optofluidic lensless-holography for detecting the composition of oil droplets," *IEEE Sensors Journal*, vol. 20, no. 13, pp. 6928–6936, 2020.

[37] M. A. Pala and M. Z. Yıldız, "Development of embedded system-based lens-less microscopy system and testing on tissue samples," *European Journal of Science and Technology*, vol. 28, no. 28, pp. 357–361, Nov. 2021.

[38] A. B. Dharmawan, S. Mariana, G. Scholz et al., "Nonmechanical parfocal and autofocus features based on wave propagation distribution in lensfree holographic microscopy," *Scientific Reports*, vol. 11, no. 1, p. 3213, 2021.

[39] G. Scholz, S. Mariana, I. Syamsu et al., "Continuous live-cell culture monitoring by compact lensless LED microscopes," *Proceedings*, vol. 2, no. 13, p. 877, 2018.

[40] Y. Wang, P. Ju, S. Wang, J. Su, W. Zhai, and C. Wu, "Identification of living and dead microalgae cells with digital holography and verified in the East China Sea," *Marine Pollution Bulletin*, vol. 163, Article ID 111927, 2021.

[41] G. Li, M. Wei, J. Sun, Y. Zhang, and R. Zhang, "Low false positive and accurate detection of yeast cell viability and concentration using an automatic staining and lensfree imaging platform," *Biochemical and Biophysical Research Communications*, vol. 525, no. 3, pp. 793–799, 2020.

[42] M. A. Pala, M. E. Çimen, A. Akgül, M. Z. Yıldız, and A. F. Boz, "Fractal dimension-based viability analysis of cancer cell lines in lens-free holographic microscopy via machine learning," *The European Physical Journal - Special Topics*, vol. 231, no. 5, pp. 1023–1034, 2021.

[43] D. Ahn, J. Lee, S. Moon, and T. Park, "Human-level blood cell counting on lens-free shadow images exploiting deep neural networks," *Analyst*, vol. 143, no. 22, pp. 5380–5387, 2018.

[44] T. O'Connor, C. Hawxhurst, L. M. Shor, and B. Javidi, "Red blood cell classification in lensless single random phase encoding using convolutional neural networks," *Optics Express*, vol. 28, no. 22, Article ID 33504, 2020.

[45] M. A. Pala, M. E. Çimen, M. Z. Yıldız, G. Güney Eskiler, and A. Deveci Özkan, "Holografik görüntülerde kenar tabanlı fraktal özniteliklerin hücre canlılık analizlerinde başarısı," *Journal of Smart Systems Research*, vol. 2, no. 2, pp. 86–94, Dec. 2021.

[46] Y. Rivenson, Y. Wu, and A. Ozcan, "Deep learning in holography and coherent imaging," *Light: Science & Applications*, vol. 8, no. 1, p. 85, 2019.

[47] Z. Ren, Z. Xu, and E. Y. Lam, "End-to-end deep learning framework for digital holographic reconstruction," *Advanced Photonics*, vol. 1, no. 01, p. 1, 2019.

[48] D. Gabor, "A new microscopic principle," *Nature*, vol. 161, pp. 777-778, 1948.

[49] W. Luo, Y. Zhang, A. Feizi, Z. Göröcs, and A. Ozcan, "Pixel super-resolution using wavelength scanning," *Light: Science & Applications*, vol. 5, no. 4, Article ID 16060, 2015.

[50] Y. Bian, W. Wang, A. Hussian, C. Kuang, H. Li, and X. Liu, "Experimental analysis and designing strategies of lens-less microscopy with partially coherent illumination," *Optics Communications*, vol. 434, pp. 136–144, 2019.

[51] T. Latychevskaia and H.-W. Fink, "Practical algorithms for simulation and reconstruction of digital in-line holograms," *Optica*, vol. 54, 2015.

[52] N. C. Lindquist, "An Introduction to Lensless Digital Holographic Microscopy," *Miniature Fluidic Devices for Rapid Biological Detection*, Springer, Cham, Switzerland, pp. 147–170, 2018.

[53] J. Zhang, J. Sun, Q. Chen, and C. Zuo, "Resolution Analysis in a Lens-free On-Chip Digital Holographic Microscope," 2019, http://arxiv.org/abs/1906.06231.

[54] G. Li, R. Zhang, M. Wei, C. Yin, J. Sun, and Y. Zhang, "Lensfree diffraction reconstruction approach enables early detection of cancer in vitro based on molecular diagnosis," *ACS Sensors*, vol. 5, no. 10, pp. 3091–3098, 2020.

[55] D. G. Voelz, *Computational Fourier Optics: A MATLAB Tutorial*, New Mexico State University, New Mexico, NM, USA, 2011.

[56] H. A. İlhan, M. Doğar, and M. Özcan, "Autofocusing in digital holography," *SPIE Proceedings*, vol. 8644, Article ID 86440C, 2013.

[57] M. Trusiak, J. A. Picazo-Bueno, P. Zdankowski, and V. Micó, "DarkFocus: numerical autofocusing in digital in-line holographic microscopy using variance of computational dark-field gradient," *Optics and Lasers in Engineering*, vol. 134, no. April, Article ID 106195, 2020.

[58] J. Mariën, R. Stahl, A. Lambrechts, C. van Hoof, and A. Yurt, "Color lens-free imaging using multi-wavelength illumination based phase retrieval," *Optics Express*, vol. 28, no. 22, Article ID 33002, 2020.

[59] H. Li, X. Chen, Z. Chi, C. Mann, and A. Razi, "Deep DIH: single-shot digital in-line holography reconstruction by deep learning," *IEEE Access*, vol. 8, Article ID 202648, 2020.

[60] E. N. Lorenz, "Deterministic nonperiodic flow," pp. 367–378, Universality in Chaos, Tyrol, Austria, 1963.

[61] Y. Tang, J. Kurths, W. Lin, E. Ott, and L. Kocarev, "Introduction to Focus Issue: when machine learning meets complex systems: networks, chaos, and nonlinear dynamics," *Chaos*, vol. 30, Article ID 063151, 6 pages, 2020.

[62] G. Quaranta, W. Lacarbonara, and S. F. Masri, "A review on computational intelligence for identification of nonlinear dynamical systems," *Nonlinear Dynamics*, vol. 99, no. 2, pp. 1709–1761, 2020.

[63] N. Tsafack, A. M. Iliyasu, N. J. De Dieu et al., "A memristive RLC oscillator dynamics applied to image encryption," *Journal of Information Security and Applications*, vol. 61, Article ID 102944, 2021.

[64] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle et al., "A 3-D multi-stable system with a peanut-shaped equilibrium curve: circuit design, FPGA realization, and an application to image encryption," *IEEE Access*, vol. 8, Article ID 137116, 2020.

[65] A. Akgül, S. Kaçar, B. Aricioglu, and I. Pehlivan, "Text encryption by using one-dimensional chaos generators and nonlinear equations," in *Proceedings of the 2013 8th International Conference on Electrical and Electronics Engineering (ELECO)*, pp. 320–323, IEEE, Bursa, Turkey, November 2013, Article ID 6713853.

[66] Q. Lai, X. W. Zhao, K. Rajagopal, G. Xu, A. Akgul, and E. Guleryuz, "Dynamic analyses, FPGA implementation and engineering applications of multi-butterfly chaotic attractors generated from generalised Sprott C system," *Pramana - Journal of Physics*, vol. 90, no. 1, pp. 6–12, 2018.

[67] K. Rajagopal, V. T. Pham, F. R. Tahir, A. Akgul, H. R. Abdolmohammadi, and S. Jafari, "A chaotic jerk system with non-hyperbolic equilibrium: dynamics, effect of time delay and circuit realisation," *Pramana - Journal of Physics*, vol. 90, no. 4, pp. 52–58, 2018.

[68] J. Liu, J. Huang, Y. Luo et al., "An optimized image watermarking method based on HD and SVD in DWT domain," *IEEE Access*, vol. 7, Article ID 80849, 2019.