IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 March 2023, accepted 17 March 2023, date of publication 31 March 2023, date of current version 6 April 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3263492

RESEARCH ARTICLE

Protection-Enhanced Watermarking Scheme Combined With Non-Linear Systems

HIRA NAZIR[1], MUHAMMAD SAMI ULLAH[1], SYED SALMAN QADRI[1], HUMAIRA ARSHAD[2], MUJTABA HUSNAIN[2], ABDUL RAZZAQ[1], AND SYED ALI NAWAZ[2]

[1]Department of Computer Science, Muhammad Nawaz Shareef University of Agriculture at Multan, Multan 60000, Pakistan
[2]Department of Information Technology, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan

Corresponding author: Muhammad Sami Ullah (samiiub@gmail.com)

ABSTRACT Communication of the images over the network calls for an approach to ensure security and ownership protection while exchanging images over the network. This paper proposes an improved blind watermarking scheme capable of offering image authentication, protection, and detachment avoidance between the watermark and its corresponding image. The proposed technique is composed of three modules; generator, protector, and resizer. The generator deals with embedding and extracting the watermark from the host image. Protector deals with encryption and decryption using a high dimensional chaotic system. And resizer deals with compressing and decompressing the watermarked image. The novelty related scientific literature is the encryption of Singular Value Decomposition (SVD) components, and watermark in a criss-cross manner using logistic map along with hyperchaotic system to achieve the confidentiality and avoid false positive problem (FPP). Whereas, embedding into RGB (red, green, blue components) is centered on singular value decomposition and level-2 Discrete Wavelet Transform. The joint operation is performed at sender's side and receiver's side, i.e., encryption, embedding, and compression is performed at sender's side whereas decompression and decryption procedures are performed at the receiver's side. Additionally, compressing the data reduces the higher bandwidth requirements. The performance of the proposed scheme is based on subjective and objective evaluation. Experimental results such as PSNR (peak signal-to-noise ratio), NC (normalized correlation), BER (bit error rate), CR (compression ratio), NPCR (number of pixel change rate), and SSIM (structural similarity index) indicate that the proposed technique approaches the standard main level The best-observed values for PSNR, SSIM, NC, and CR are 73.2211, 0.998816, 0.9997, and 0.9025 respectively.

INDEX TERMS Watermarking, decomposition, non-linear dynamics, confidentiality, logistic.

I. INTRODUCTION

Dispensing personalized healthcare using IoT-based architectures, artificial intelligence, and 5G-based networks is shifting the world towards Health 4.0 [1]. Security of medical images embedded with sensitive data is a significant issue in transferring medical data. Information and Communications Technology (ICT) tools to manage, store, and transmit medical data facilitates patients to get health care services by exchanging their medical records over long distances. These services may suffer from authenticity and confidentiality issues. Since medical data may become susceptible during storage and transmission; therefore, its security and privacy must be built into the algorithm. And the providers must guarantee the authenticity and confidentiality of the sensitive patients' data through watermarking and encryption. Otherwise, the belonging of the specific media will be adversely affected. The security of personalized images or certain medical information contained in some host images, illegal possessions, and ownership protection are the issues from the perspective of communication networks. Moreover, identity theft, privacy leakage, and authenticity related to medical data are a growing issues [2], [3]. Acronyms listing used in this paper is shown in Table 1.

The associate editor coordinating the review of this manuscript and approving it for publication was Yilun Shang.

Efficient security protocols are desperately needed to cope with the severity of data breaches in the healthcare industry. Although, cryptographic algorithms can be used to safeguard the Electronic Health Records (EHRs), the camouflaged presence of encrypted multimedia data fascinates more attention from the invader, thereby increasing the possibility of data breaches.

Conversely, embedding the EHRs in medical images by using invisible watermarking algorithms has been an efficient way of improving the security of multimedia data. Therefore, the highly imperceptible watermarking techniques can lead to a reduced number of privacy breaching chances by an adversary.

Steganography deals with secretly transmitting the piece of information by embedding it into some trivial cover image [4], [5]. Although, steganography deals with data confidentiality whereas, invisible digital watermarking offers other benefits such as (a) confirmation of content creator, (b) non-susceptibility to illegal distribution, copyright breach problems, and alteration while sending data over the internet. However, it is seen that integrating an encryption algorithm with an invisible watermarking algorithm can generate highly secured watermarked data [6]. Therefore, integrating water marking with encryption algorithms can tackle the challenging issues related to copyright infringement, image watermarking attacks, and information security.

Digital image watermarking schemes embed a secret watermark image into the host image using spatial or frequency domain. The secret watermark image can be encrypted before embedding it into a host image. For example, the author [7] first encrypts the watermark image, then embeds it into the host image. Commutative watermarking-encryption proposals implemented by various researchers in the recent past, are comprised of two main parts, i.e., an encryption and watermarking part. The encryption part uses a spatial or transform domain to encrypt the watermark bits by exploiting encryption procedures such as permutation-substitution. Whereas watermarking part is comprised of watermark key W_K, the watermark W, dimension of host vector and watermarking procedure. In this respect, commutative watermarking-encryption based scheme performs encryption in the spatial domain by using permutation, and accomplishes watermarking by exploiting the watermark key W_K, the watermark W, dimension of host vectors (the number of coefficients, which is used for embedding one bit) and the quantization step Δ [8].

Maintaining an appropriate balance between robustness and imperceptibility has always been a demanding factor. Besides, other factors to be considered while designing watermarking schemes are: balance between fidelity and reversibility, space efficiency, watermarking in encrypted domain, payload capacity, and reduced size of the watermarked data. The issue of delegating the multimedia watermarking service to cloud service providers is tackled in [9], in which the authors achieve a notable balance between reversibility and fidelity under the specified constraints. Additionally, it substantially reduces the size of the watermarked image and improves the space efficiency.

Although, Singular Value Decomposition (SVD) based image watermarking techniques offer remarkable invisibility but suffer from False Positive Problem (FPP). The procedures that are centered on SVD method decompose the transformed image into U, S, and V vectors. Embedding is done into one of these vectors. The S vector is mainly utilized for embedding owning to its robust nature against certain attacks [10]. Furthermore, a minor modification in singular vectors does not affect the host image's visual quality.

Conversely, in image watermark insertion, false positive problem results from singular values of SVD. The vectors U and V can be interchanged by the adversary's chosen matrices for the extraction of new watermark (that has never been embedded) to appeal the false ownership. By encrypting the SVD components through one way hash functions and non-linear dynamics, the FPP problem can be avoided [11], [12]. The author in [11], tackled the FPP problem by encrypting the SVD components via a Logistic map. Therefore, connecting watermarking scheme with encryption based on non-linear dynamics can generate a highly secured watermarked image [13], thereby reducing the false positive problem and other security issues. To that end, a novel watermarking procedure is formulated that connects the watermarking part with encryption based on Arnold transform by using the inter-block coefficient correlation for embedding purposes [14]. In this scheme, the author improves the security by resisting image processing and geometric attacks.

The objective of the conducted research is to embed multiple size image watermarks in the cover image, and 2) to include encryption of embedded watermarks using hyperchaotic system to avoid the false positive problems i.e., if intruder becomes successful in extracting the watermark, he/ she will not be able to understand it or claim ownership as it is in encrypted form using higher dimensional chaos. If the intruder claims watermark ownership, he/ she will have to decrypt it.

Specifically, in this study, a blind color image watermarking scheme that combines second-level discrete wavelet transform (DWT), singular value decomposition (SVD), encryption procedure, and compression technique to provide security for watermarked images. Before embedding the required watermark into the host image, it is encrypted by using a hyperchaotic system in a novel way, and, the encryption of SVD components is also done using a logistic chaotic map to get around the false positive problem. Subsequently, the watermarked image is compressed to decrease the bandwidth requirement. Hence, the significant contributions of the proposed scheme are: (a) a good balance of trade-off between imperceptibility and robustness with the numerous size image watermarks is attained, (2) dual encryption, i.e., encryption

TABLE 1. List of acronyms.

Acronym	Full Form	Acronym	Full Form
PSNR	Peak to Signal Noise Ratio	C_{img}	Cover Image
WKD_{img}	Watermarked Image	W_{img}	Watermark Image
C_{data}	Compressed Data	RC_{img}	Recovered Cover Image
SVD	Singular Value Decomposition	$EncW_{img}$.	Encrypted Watermarked Image
EW_{img}	Extracted Watermark Image	BER	Bit Error Rate
2DWT	Second Level Discrete Wavelet Transform	CR	Compression Ratio
EHR	Electronic Health Record	OCT	Optical Coherence Tomography
DICOM	Digital Imaging and Communications in Medicine	LZW	Lempel–Ziv–Welch
DCT	Discrete Cosine Transform	PC	Principal Component
ABC	Artificial Bee Colony	NC	Normalized Co-efficient
IWT	Integer Wavelet Transform	HVS	Human Visual System
FPP	False Positive Problem	LE	Lyapunov Exponent

of SVD components based on Logistic map and encryption of watermark based on a hyperchaotic system in a criss-cross manner.

The rest of the proposed work is structured as follows. Preliminaries are given in section II. Related research is presented in section III, and proposed work related to embedding, encrypting/ decrypting, compressing, and extracting is given in section IV. Performance analysis of the proposed technique is given in section V. Finally, concluding remarks along with the future objectives, are given in section VI.

II. PRELIMINARIES

A. DISCRETE WAVELET TRANSFORM

Discrete wavelet transformation (DWT) has widespread applications ranging from detection of organ's diseases to digital multimedia security [15]. The elementary sense of DWT in image processing is to pass an image through series of high and low-pass filters to create higher and lower frequencies i.e. decomposing the image into 4 non-overlapping frequency sub-bands namely, low-frequency sub-band called as (LL), mid-frequency sub-band called as (LH, HL), and high-frequency sub-band called as (HH). LL sub-band is acquired by passing a host image through low-pass filter in both directions i.e., row wise and column wise. LL sub-band possesses most of the information about the original image and specifies rough approximation about the original image. Likewise, high pass sub-band i.e., HH sub-band is acquired by passing an image through high pass filter in both directions. Whereas, to get HL along with LH sub-band, the original signal is passed through two filters i.e., high-pass followed by low-pass filter and vice versa in both directions. Any one of the 4 sub-bands can be taken for further

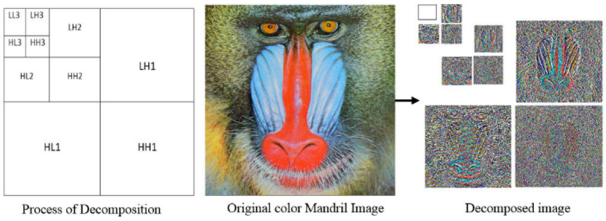

FIGURE 1. Decomposition of a color image up to three levels. Here white square in the decomposed image represents the level 3 i.e., LL3 sub-band.

transformations. Here we take the LL sub-band for further transformations as it provides resistance to various attacks. Each one of these sub-bands behave like a filter against signal processing attacks such as Gaussian noise, Salt & Pepper noises, Histogram equalization, Blurring, Sharpening, Median and Average filtering. Besides, DWT exhibits an isotropic trait of the Human Visual System (HVS) higher than other transformation processes such as Fast Fourier Transform (FFT) or Discrete Cosine Transform (DCT). This specification aids in the invisibility of embedded watermarks in less sensitive regions by HVS [16]. Thus, the robustness of the watermarked image is enhanced without deterioration of the image quality. Thus, owing to the low-pass features of the LL sub-band, the embedding into this sub-band provides resistance to various attacks such as distortion, loss of compression, and geometric distortions.

Additionally, the embedding in this sub-band will have a nominal influence on the original image but the capacity becomes less than a quarter of the original image size. In Fig. 1, DWT transforms the original cover image into 4 separate sub-bands (LL, HL, LH, and HH) up to 3 levels. The LL, HL, LH, and HH sub-bands deal with approximation, horizontal, vertical, and diagonal details respectively, where H denotes high pass filter, and L denotes low pass filter. The three sub-bands i.e. LH, HL, and HH are called detail components which comprise high frequencies and are considered the most appropriate for watermark embedding with more excellent stability and robustness [17]. The DWT is a reversible transformation. The inverse DWT reconstructs the original image from the wavelet domain into the spatial domain by using approximation and detail coefficients. Therefore, the inverse DWT is a way to reconstruct the original signal or image from the approximation and detail coefficients obtained through DWT. The 2-dimensional decomposition of an image up to level-1 into its sub-bands and reconstruction is shown in Fig. 2.

B. SINGULAR VALUE DECOMPOSITION

Suppose $\boldsymbol{A}$ is a matrix of size $\boldsymbol{M} \times \boldsymbol{N}$ consisting of real numbers. The SVD procedure on $\boldsymbol{A}$ produces two orthogonal, unitary matrices i.e., $\boldsymbol{U}(\boldsymbol{M} \times \boldsymbol{M})$ and $\boldsymbol{V}(\boldsymbol{N} \times \boldsymbol{N})$, and one diagonal matrix, i.e., $\boldsymbol{S}(\boldsymbol{M} \times \boldsymbol{N})$ and can be stated as [18]:

$$\boldsymbol{A} = \boldsymbol{USV}^{\boldsymbol{T}}. \tag{1}$$

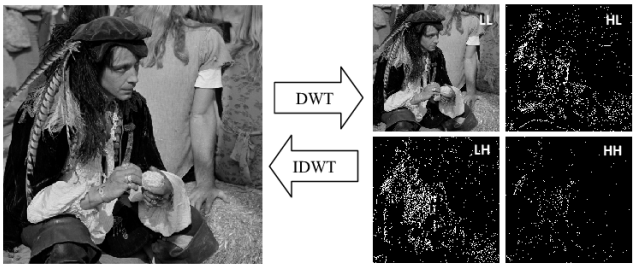

FIGURE 2. First-level decomposition using DWT and image reconstruction using inverse DWT.

The diagonal matrix $\boldsymbol{S}$ represents the singular values ($\boldsymbol{\sigma_i}$) of matrix $\boldsymbol{A}$ in descending order, i.e., ($\boldsymbol{\sigma_i} > \boldsymbol{\sigma_{i+1}}$). SVD can be applied to color and grayscale images of size $\boldsymbol{N} \times \boldsymbol{N}$ or $\boldsymbol{M} \times \boldsymbol{N}$. Any minor modifications in the singular values doesn't cause significant effect on an image's visual quality [19]. SVD procedure reduces an image of size $\boldsymbol{M} \times \boldsymbol{M}$ or $\boldsymbol{M} \times \boldsymbol{N}$ into smaller square and invertible matrices. The unitary property of $\boldsymbol{U}$ and $\boldsymbol{V}$ matrices and stability property of singular value matrix makes it useful in image invisible watermarking approaches. But SVD based approaches also induce False Positive Problems –FPP (extracting the illegal or non embedded watermark images from the watermarked images to claim the false ownership is called as FPP) [20]. The singular values of the diagonal matrix $\boldsymbol{S}$ are used for embedding the watermark into the host image by using an optimized scaling factor. The SVD components $\boldsymbol{U}$ and $\boldsymbol{V^T}$ are used in the extraction process as they provide the geometric information. If these components are not encrypted, then they can cause FPP. Therefore it is necessary to encrypt these components to avoid the FPP [11]. Hence, encryption of these components, i.e., $\boldsymbol{U}$ and $\boldsymbol{V^T}$ Serves as an additional layer of security against FPPs.

C. WATERMARK ENCRYPTION

Encryption along with Compression helps securely transfer the image data over the insecure network with less bandwidth requirement. Protection and compression of image data at the sender's side are assured by encryption and compression procedures. The joint operation, i.e., decompression and decryption, are performed at the receiver's side. In our research study, the encryption is based on a chaotic and hyperchaotic systems whereas LZW is employed as a lossless compression technique for compressing the text or image data. The chaotic system used in this study is given as:

$$X_{n+1} = \beta X_n(1 - X_n). \tag{2}$$

Here, X_n denotes system variable with n number of iterations, and β denotes control parameter. For $3.56 \leq \beta \leq 4$, (2) shows chaotic behavior and generates a set of random numbers that can be used for scrambling the watermarks. Whereas the four-wing hyperchaotic system [21] used in this study is given as:

$$\begin{cases} \dot{x}_{n+1} = ax_n + byz \\ \dot{y}_{n+1} = cy_n + dx_nz \\ \dot{z}_{n+1} = ex_ny_n + kz_n + mx_nw_n \\ \dot{w}_{n+1} = ny_n. \end{cases} \tag{3}$$

where x, y, z, w are the state variables, and a, b, c, d, e, k, m, n signify the system parameters. Equation (3) with $a = 8$, $b = -1$, $c = -40$, $d = 1$, $e = 2$, $m = 1$, $n = -2$, $k = -14$ becomes hyperchaos, i.e., it has two positive Lyapunov exponents (LEs). Its LE1=1.39, LE2=0.50, LE_3=0, and LE_4=−47.9. Moreover, the visual representation of the system attractor of (3) shown in Fig. 3 indicates that the sequences generated by the system are more chaotic.

Chaotic systems exhibit non-linear behavior and are characterized by a sensitive dependence on initial conditions, and pseudo randomness [22], [23]. On the contrary, the hyperchaotic system owns more complex pattern, larger key space, and randomness. Mathematically, the behavior of chaotic and hyperchaotic systems can be identified by computing Lyapunov Exponents (LEs). Chaotic systems have only one positive LE, while hyperchaotic systems have two or more positive LEs. LE can be computed by using (4) and is defined as the average logarithmic rate of separation or convergence between the two points on the orbits at time series t. Briefly, LE is the exponential separation rate for two nearby trajectories of a dynamical system [24].

$$LE = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln \left| \frac{\Delta D_i}{\Delta D_o} \right|, \tag{4}$$

where $\boldsymbol{\Delta D_o}$ is the initial difference between the two initial conditions $\boldsymbol{X_o}$ and $\boldsymbol{Y_o}$. If the non-linear system has two or more Positive Lyapunov Exponents (PLEs), it is called hyperchaos, and they show much more complicated behavior as compared to chaotic systems. In the Fig. 4, the encrypted image is compressed using a dictionary-based compression technique called Lempel-Ziv-Welch (LZW) compression [25]. The code length, for this compression technique is usually fixed and there is no need for additional information to decompress the data.

III. RELATED WORK

Watermarking schemes having robustness, imperceptibility, and security features are discussed in this section. A highly imperceptible watermarking scheme that combines SVD and fast curvelet transform to embed EHR into OCT scans is presented [26]; this scheme also resists some image processing attacks. DWT-based only watermarking schemes have shown better imperceptibility and compression, but these schemes do not resist geometric attacks to a great extent [27]. Hence, these schemes are usually joined with SVD or Hessenberg decompositions to make them more robust [11]. An innovative approach proposed by [28] applies DWT decomposition

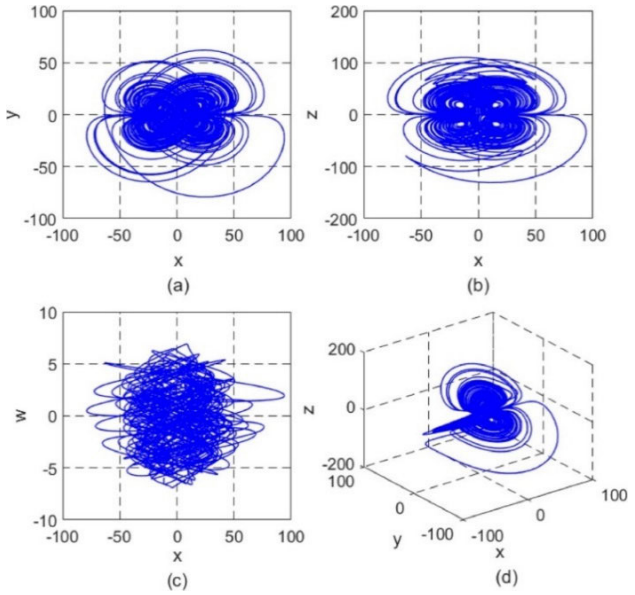

FIGURE 3. The system attractor.

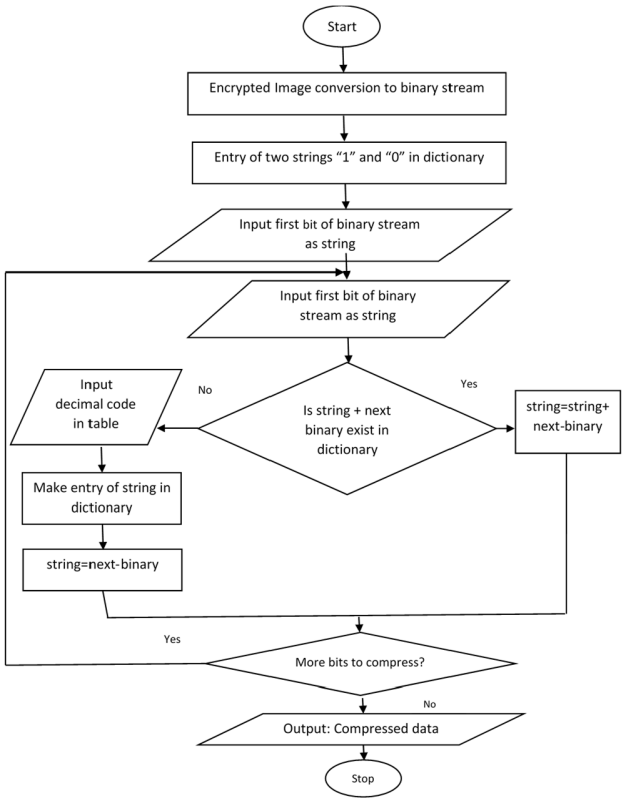

FIGURE 4. Compression workflow.

in an appropriate way, i.e., it makes adjustments during insertion. Afterward, the implementation of SVD to LL, LH, and HL sub-bands yields three singular value matrices that are used for watermark embedding. The proposed approach certifies data integrity, along with confidentiality, and robustness for image processing attacks. In the interest of maintaining a high-quality watermarked image, enhancing the security and ensuring the data integrity, an approach was proposed by [29] adds the hash of Electronic Patient Record (EPR) to the original watermark. Afterward, a DWT is applied to the medical image, then an SVD is implemented to the LL sub-band. Then watermark is integrated into the least significant part of the particular component. A watermarking embedding and extracting scheme proposed by [30] uses a dual transform domain, i.e., SVD and DCT, followed by a chaos-based encryption to avoid the false positive problems. In addition to watermark embedding, the author [31] presents a color image watermarking procedure centered on a fast structure-preserving algorithm of quaternion singular value decomposition (QSVD). This scheme is effective in invisibility and confidentiality, and is robust to certain image processing attacks. Likewise, the watermarking schemes proposed by [32], [33], and [34] encrypt the watermark bits by exploiting hyperchaotic maps before embedding into host image. A blind watermarking scheme proposed by [32] makes use of Fractional Moments of Charlier–Meixner for computing and embedding the watermark bits into the host image. This scheme demonstrated a better trade-off between robustness and imperceptibility. The random projection approach implemented by [33] achieves higher imperceptibility and robustness against filtering and geometric attacks. By combining FFT and DCT in the wavelet domain, the watermarking scheme exhibited better invisibility and robustness against geometric attacks [27]. The authors in this scheme got a security component by exploiting dual encryption. An invisible blind watermarking procedure proposed by [34] successfully authenticates the patients' images embedded with EHRs. A new digital watermarking scheme based on multiple modules, i.e., orthonormal restoration, level shifting, distortion compensation, etc., significantly improves robustness at a higher level of imperceptibility by overcoming the flaws of existing SVD-based schemes [35].

Alternatively, the authors in [36] diffused the watermark and host images using Arnold's chaotic map. And the principal component (PC) of diffused host image is achieved through redundant DWT and SVD. Afterward, diffused host image's PC is embedded with diffused watermark bits by exploiting adaptive scaling factors optimized through Artificial Bee Colony. The adaptive scaling factors accomplished better invisibility with improved robustness and security. Apart from using a single transformation, connecting the multiple transformations such as SVD, DFT, LWT and DCT bettered the imperceptibility and robustness but resulted in high computational complexity [37]. Similarly, including scaling factor optimization algorithms such as Cuckoo search [38], firefly algorithm [39], Artificial Bee Colony (ABC) [40], Particle Swarm, Fruit Fly optimization and Whale optimization algorithms in the watermarking scheme achieves better trade-off between robustness and imperceptibility. The author in [41] exploited Wang Landau WL based optimization followed by SVD and wavelet transform up to

three levels. By doing so, the author got better embedding coefficient.

To achieve a better trade-off between imperceptibility and robustness against specific attacks, the watermarking scheme given by [42], exploited Arnold transform, SVD, DWT, and finally Differential Evolution (DE) for scaling factor optimization. This scheme achieves remarkable invisibility as the luminance component is elected for watermark embedding because the HVS is insensitive to this component; hence, embedding watermark bits into this component will definitely enhance invisibility. A secure and acceptable robustness with excellent invisibility is achieved by exploiting the combination of DWT, IWT, Contourlet Transform and 3D Henon map [43]. A color watermarking scheme based on numerous Fourier transform variants is proposed [44]. This scheme is based on the combined parity of coefficients and embeds watermark bits in the medium frequency band. And achieves PSNR$\geq$40db with resistance to specific attacks up to a certain threshold level. Another watermarking scheme is based on two parts, i.e., generator and adversary. The generator deals with producing the watermarked images by embedding the watermark bits into the mid-frequency region and extracting the watermarks from the watermarked images polluted with noise. The adversary part pollutes the watermarked image by adding particular noise. This scheme has shown better visual performance and robustness against noise intrusion [45]. The text watermarking method proposed by [46] exploits the reversing technique to enhance the security of Arabic Text in the Holy Quran by using vowels with kashida. The proposed approach achieves an embedding ratio of about 90.05% and a high imperceptibility (PSNR) of 72.33 dB approx. The sensitive data of patients such as blood pressure, lipid profile and other health related information is concealed in the host image using IWT along with standard deviation block (SD-block), least significant bit replacement, and coefficient alignment technique. The results confirmed high hiding storage, high imperceptibility, and a certain degree of robustness with low time complexity [47].

In order to achieve a good balance between imperceptibility and robustness, Discrete Cosine Transform (DCT) and Schur decomposition is exploited in first scheme whereas, DWT along with Schur Decomposition offers more robust watermark distribution. Tabulated results reveal that the proposed schemes maintain a high quality watermarked images and are very robust against various attacks [48]. DWT and SVD is applied to embed and extract the image watermark into the patient's image with satisfactory adjustment during the insertion. The proposed scheme confirms data integrity, confidentiality, and robustness to several conventional attacks [28]. A semi-fragile approach proposed by [49] reveals the acceptable imperceptibility and robustness to certain attacks even though controlling the watermark integrity. Limitations of the previous work are reported in the Table 2.

TABLE 2. Limitations in previous work.

Reference	Proposed Scheme	Limitation
[26]	A highly imperceptible watermarking scheme that combines SVD and fast curvelet transform to embed EHR into OCT scans.	This scheme only resists image processing attacks and doesn't use multiple size image watermarks.
[27]	DWT-based only watermarking scheme shows better imperceptibility and compression.	This scheme doesn't resist geometric attacks.
[28]	An innovative approach makes use of DWT decomposition in an appropriate way, i.e., it makes adjustments during insertion. Afterward, the implementation of SVD to LL, LH, and HL sub-bands, it yields three singular value matrices that are used for watermark embedding.	This scheme only resists image processing attacks and uses fixed size image watermarks for embedding.
[29]	The proposed approach adds the hash of Electronic Patient Record (EPR) to the original watermark. Afterwards, a DWT is applied to the medical image, then an SVD is implemented to the LL sub-band. Then watermark is integrated into the least significant part of the particular component.	Doesn't offer higher watermark embedding capacity.
[30]	The proposed watermarking embedding and extracting scheme uses a dual transform domain, i.e., SVD and DCT, followed by a chaos-based encryption to avoid the false positive problems.	Doesn't offer higher watermark embedding capacity. Only embeds fixed size gray level watermark images.
[31]	This scheme presents a color image watermarking procedure centered on a fast structure-preserving algorithm of quaternion singular value decomposition (QSVD).	Although achieves good imperceptibility, and robustness to various attacks but doesn't support multiple size colored watermarks for embedding. Doesn't encrypt QSVD components. Simulation for false positive problem is not presented.
[33]	The random projection approach implemented by achieves higher imperceptibility and robustness against filtering and geometric attacks.	Suffers from false positive problem. Unable to retrieve the manipulated regions.
[34]	A digital watermarking scheme composed of invisible and zero watermarking procedure successfully authenticates the patients' images embedded with EHRs. It is reliable and secure. And exhibits high robustness against all image compression modes, filtering, noise, image enhancement and geometric distortions.	Although establishes a proper link between embedded EPR, and medical image but whenever manipulated region is extracted the NC value of extracted watermark image drops. Cover images of size 512×512 are used for embedding.
[35]	A new digital watermarking scheme based on multiple modules, i.e., orthonormal restoration, level shifting, distortion compensation, etc., significantly improves robustness at a higher level of imperceptibility by overcoming the flaws of existing SVD-based schemes.	Although, the scheme offers better imperceptibility, robustness against various attacks but incurs highest computational overhead while performing the composite operations of level shifting, SVD, and sign correction. The overall complexity of $N \times N$ pixels image is $O(12n^3 + 6n^2)$.

TABLE 2. *(Continued.)* **Limitations in previous work.**

[36]	The authors diffused the watermark and host images using Arnold's chaotic map. And the principal component (PC) of diffused host image is achieved through redundant DWT and SVD. Afterward, diffused host image's PC is embedded with diffused watermark bits by exploiting adaptive scaling factors optimized through Artificial Bee Colony	The NC values for robustness remains in between [0.65-0.8] for cropping 50% attack. 24 bit 512×512 color images are used as cover images whereas, fixed sized images of size less than cover images are used as watermarks. Although, it is free from false positive error but whenever the watermarked image is manipulated, the extracted watermark's NC value suddenly drops from 0.99 to ≈0.7.
[50]	A robust network flow watermarking method based on **Hetero**geneous **T**ime **C**hannels (named as HeteroTiC), which is designed to surmount the shortages of watermarking with a single packet feature and static configurations. Three time channels (packet order, packet timing and packet size) are integrated deeply to carry watermark.	Doesn't compress and encrypt the watermark or watermarked media. Uses fixed size watermarks for embedding.
[51]	Proposed scheme is based on DWT-SVD in Fractional Order Fourier Transform (FRFT) domain.	Gray scale cover and watermark images of size 512×512, and 128× 128 respectively are used in simulation. Normalized Correlation drops to 0.800 for Gaussian noise (m=0, v=0.01).
[52]	Fragile watermarking schemecentered on Integer-to-Integer Discrete Wavelet Transforms (IIDWT) and A5 Lattice Vector Quantization (LVQ) is proposed. Metadata along with Message Authentication Code (MAC) is embedded into the medical image.	Whenever the Bits Per Pixel (BPP) is increased, the values of PSNR decrease and impose more distortion. (The BPP can be computed by dividing the number of embedded secret bits to the total number of pixels in the cover image).

IV. PROPOSED APPROACH

The proposed scheme consists of three parts at the sender's side, and three parts at the receiver's side, i.e., watermark embedding, encryption, and compression at the sender's end, whereas decompression, decryption, and extraction are done at the receiver's end. First, decomposition up to second level Discrete Wavelet Transform of the cover image is performed. Discrete Wavelet Transform transforms the original cover image into 4 separate sub-bands (LL, HL, LH, and HH) up to two levels. The two levels of DWT are given in Algorithm-1 (step-1). The LL, HL, LH, and HH sub-bands deal with approximation, horizontal, vertical, and diagonal details, respectively, where H denotes high pass filter, and L denotes low pass filter. The three sub-bands, i.e., LH, HL, and HH, are called are detail components comprising high frequencies and considered the most appropriate for watermark embedding with, excellent stability and robustness.

The singular component of the intermediate frequency sub-band, i.e., $\boldsymbol{LH1}$ of the first level Discrete Wavelet Transform coefficients, is embedded with the given color watermark image. Finally, inverse SVD and DWT procedures are applied to get the watermarked image. Another aspect that can present a very critical security situation to the owners of the media contents in proving their rightful ownership is the false positive problem in which attackers claim the false ownership of media contents. The SVD components i.e. $\boldsymbol{U_{LH1}}$ and $(\boldsymbol{V_{LH1}})^{\boldsymbol{T}}$ are also encrypted with the 2D Logistic map [50] given in (2) to avoid the false positive problem (in which attackers appeal the false ownership of media stuffing); that is, if an intruder gets forged SVD components, then the intruder could only extract a scrambled watermark which is not recognizable by the human visual system. (2) shows chaotic behavior and generates a set of random numbers which are used for scrambling the SVD components.

Control parameter specific values along with the initial conditions are input to the non-linear differential equation i.e., (3), then it is solved by using 4th order Runge Kutta method to obtain the random sequences x, y, z, w and all these four sequences are combined in to form an array. Control parameter specific values determine the behavior of non-linear differential equation either chaotic, hyperchaotic or not. Initial condition values may be generated from some random source or can be given manually in any range. One set of initial conditions values exhibit a very different hyperchaos behavior as compared to the other set of initial condition values having 1-bit difference. Before embedding, the watermark image is encrypted by using the random sequences x, y, z, w generated by a higher dimensional chaotic system given in (3), which shows hyperchaotic behavior when $\boldsymbol{a = 8}$, $\boldsymbol{b = -1, c = -40, d = 1, e = 2, m = 1, n = -2, k = -14}$. Moreover, the binary sequences generated by (3) also passed (NIST) SP800-22 [54], comprising 15 randomness sub-tests which designates that (3) is suitable for providing confidentiality to the watermarked images. Afterward, the encrypted watermarked image is compressed using LZW compression and is ready to be delivered over a communication channel. The specific steps for watermark encryption and watermark embedding are given in Algorithms 1 and 2. The complete watermark embedding, encryption, and compression flowcharts are shown in Fig. 5, 6, and 7.

Fig. 7 represents the extraction process on the receiver's side. The compressed data is decompressed, extracted by performing the inverse steps of algorithms 1, and 2 in the reverse order, and finally, the decryption procedure is executed to get the watermark. For the sake of understanding, an example of a system model is presented in Fig. 8 below. In this figure, a reference standard color image and watermark are taken and passed through the proposed algorithms.

Algorithm 1 Encrypt Watermark

Input: Image watermark W_{img}, specific values of control parameters, and initial conditions as input in (3).

Output: EW_{img}. (Image watermark in encrypted form)

Step 1. Solve 4D Hyperchaotic System (3) by using initial conditions and control parameters to produce an array of a random sequence R_{seq}.

Step 2. Compute an array N by adding the constant number C_o ranging from 0 to 255 to each value of R_{seq} then take mod to produce key K.

$$add\left(C_o, R_{seq}(i)\right) \Longrightarrow N$$
$$mod\left(N, 256\right) \Longrightarrow K$$

Step 3. Perform XOR between W_{img} and K to get 1st stage encrypted watermark image Est_{img}.

$$XOR\left(W_{img}, K\right) = FEW_{img}.$$

Step 4. Now compute the mean intensity value M_{val} of FEW_{img} and compute the modified key K'.

$$Mean_{intensity(FEW_{img})} \Longrightarrow M_{val}.$$
$$add\left(M_{val}, R_{seq}\right) \Longrightarrow N'.$$
$$mod\left(N', 256\right) \Longrightarrow K'.$$

Step 5. Perform XOR operation and get EW_{img} by using K'.

$$XOR\left(FEW_{img}, K'\right) \Longrightarrow EW_{img}.$$

Thus, a watermarked image is generated, and sent to the receiver through the network. The proposed technique is blind as it doesn't need original watermark and host images for the extraction of a watermark. Therefore, the receiver only gets the watermarked image and can extract the embedded information. Then, the extracted information is decrypted to produce a watermark similar the original watermark.

V. RESULTS AND ANALYSIS

In order to conduct experiments, we used hundred different cover images (512×512) and watermark images (256×256) taken from publically available image database Medpix (https://medpix.nlm.nih.gov/home) and USC-SIPI (https://sipi.usc.edu/database). All the simulations are performed on MATLAB R2017a installed on windows 10, 64-bit operating system with an i7 processor, 8GB RAM, and 2.4GH clock speed. Some sample images used for simulating experiments are shown in Fig. 9, whereas watermark images are shown in Fig. 10. Performance of the proposed blind watermarking scheme is based on objective and subjective methods. Details of standard metrics (objective measures) used for evaluation are listed in Table 3. In the proposed blind watermarking scheme, a watermarked image along with

Algorithm 2 Embedding

Input: Cover Image C_{img}, Encrypted watermark image EW_{img}, Text watermark.

Note: (The two-dimensional units, i.e., blue, green, and red channels of an image C_{img} are separately passed as two-dimensional units to the DWT and SVD, and in the end, these two-dimensional units are merged to form a sub-band of the color image. For example, $LL1$ in step 1 (Algorithm-2) denotes the merged sub-band of a transformed color image, i.e., representing a three-dimensional unit).

Output: Compressed data C_{data}.

Step 1: Apply second-level DWT on a cover image C_{img} of size M×M where M=32, 64, 128, 256, 512, 1024 etc.

$$DWT\left(C_{img}\right) \Longrightarrow [LL1, HH1, HL1, LH1].$$
$$DWT\left(LL1\right) \Longrightarrow [LL2, HH2, HL2, LH2].$$

Step 2: Apply the SVD procedure on the sub-bands created in step 1.

$$SVD\left(LH1\right) \Longrightarrow [U_{LH1}, S_{LH1}, V_{LH1}].$$

Step 3: Read the watermark image EW_{img}.

Step 4: Do watermark embedding into the singular matrix S_{LH1} by using a gain factor α.

$$ES_{LH1} \Longleftarrow \left[S_{LH1} + \alpha \times EW_{img}\right].$$

Step 4: Apply the SVD procedure inversely to get the DWT sub-bands of watermarked image.

$$E_{LH1} \Longleftarrow U_{LH1} \times ES_{LH1} \times (V_{LH1})^T.$$

Step 4.1: Iterate the Logistic map to produce two one-dimensional vectors $T1$ and $T2$ and transform them into two-dimensional vectors $UT1$ and $VT2$ and perform encryption to get two encrypted vectors denoted by mU_{LH1}, mV_{LH1}.

$$XOR\left(U_{LH1}, UT1\right) \Longrightarrow mU_{LH1}$$
$$XOR\left((V_{LH1})^T, VT2\right) \Longrightarrow (mV_{LH1})^T$$

Step 5: Read the text watermark t_w of a certain length (up to 255 characters), convert it into a binary watermark b_w and embed it into the $HH2$.

binary('text_watermark') $\Longrightarrow b_w$
embed_txt$(HH2, b_w, L, \alpha_1) \Longrightarrow b_w HH2$

Here, L and α_1 signify the length of b_w and the gain factor in embedding the text watermark.

Step 6: Perform inverse DWT to get a watermarked image WKD_{img}.

$$InverseDWT\left(LL2, HL2, LH2, b_w HH2\right) \Longrightarrow ILL1.$$
$$InverseDWT\left(ILL1, LL2, E_{LH1}, HH1\right) \Longrightarrow WKD_{img}.$$

Step 7: Perform compression by using LZW or Huffman technique to get compressed data C_{data}.

$$compression\left(WKD_{img}\right) \Longrightarrow C_{data}.$$

Algorithm 3 Extraction

Input: compressed data C_{data}.

Output: Extracted watermark image XW_{img}, recovered watermark RW_{img}, text watermark and recovered cover image RC_{img}.

Steps: Algorithms 1, 2 are executed in reverse direction.

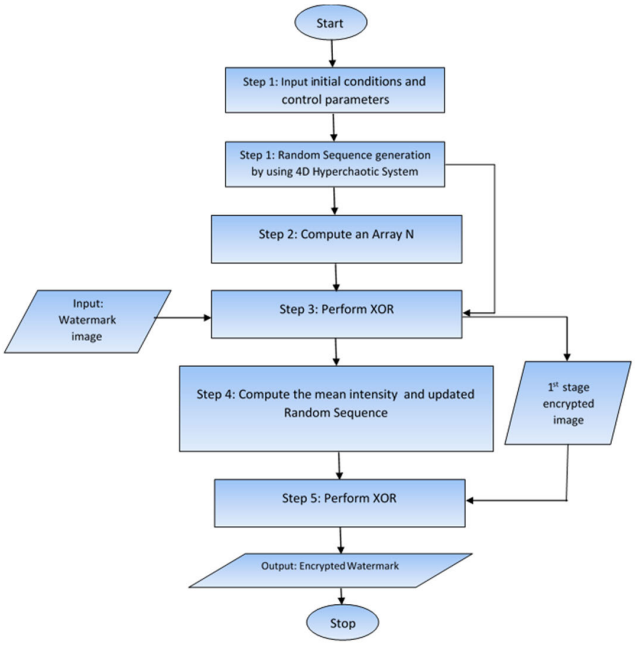

FIGURE 5. Watermark encryption workflow.

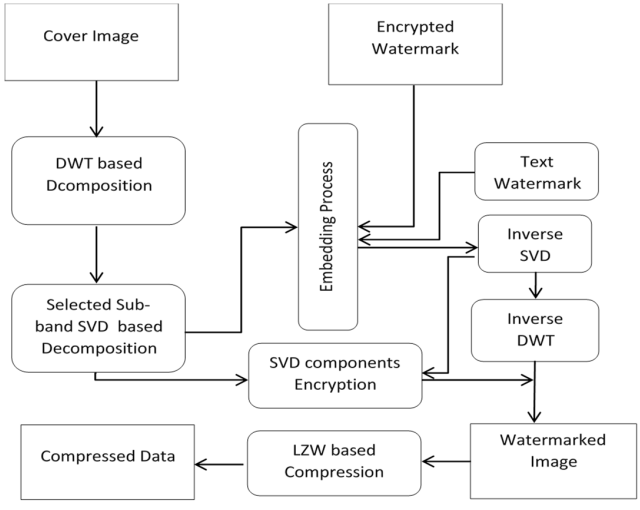

FIGURE 6. Watermark embedding workflow.

a key is used for watermark extraction because in blind-watermarking schemes, there is no need for original watermark and host images for the extraction of the watermark. Whereas non-blind watermarking schemes demand an original cover images aside from the key and watermarked images for extracting the embedded watermark [55].

The proposed watermarking scheme for various images is simulated by exploiting various gain factors α as [0-0.2], but the optimum performance in terms of PSNR, NC, BER, SSIM, and Compression Ratio (CR) was found at $\alpha = 0.115$. The performance indicators are shown in Table 4. The best-observed values for PSNR, SSIM, NC, and CR are 73.2211, 0.998816, 0.9997, and 0.9025, respectively. We have also computed the average values by testing the proposed scheme on 100 dissimilar medical images as shown in Table 5. The subjective measure is based on the visual simulation, i.e., qualitative analysis. The best quality watermarked image is obtained at the main factors in the range of [0.11-0.2]. The watermarked image quality degrades beyond this range. Robustness values against specific attacks shown in Table 6 indicate that the proposed scheme is robust against JPEG compression, median filter, histogram attacks, salt & pepper noise, and speckle noise.

The proposed schem's robustness is compared to some recently published watermarking schemes. The comparison based on specific attacks is shown in Table 7. It is observable that NC values are better under specific attacks while comparable in the majority of the cases. The results of imperceptibility between the host and watermarked image are listed and compared in Table 8. It is obvious that the imperceptibility values are better in some cases and comparable in most cases. Table 9 displays the average computational time regarding watermark embedding time, watermarked-image encryption time, compression time, decompression time, watermarked-image decryption time, and watermark extraction time. The average computational time is tested by taking cover images having dimension (512×512) from Medpix image database while the three images having dimensions 256×256, 128×128, and 64×64 are used as image watermarks.

To assess robustness under specific attacks associated with various parameters, we used cover images having dimensions 512 × 512 and watermark images having dimensions 256 × 256, 128 × 128, and 64 × 64. The computed NCs under certain attacks are shown in Fig. 11. In Fig. 11 (a), the NCs under JPEG2000 compression remained above 0.8 up to the compression ratio of 36. The NCs for watermark images having dimensions 256 × 256 and 128 × 128 in Fig. 11 (b) under JPEG compression crosses 0.9 as the QF approaches 45. The NCs in Fig. 11 (c) remain above 0.8 up to the sigma 4.5. The NCs in Fig. 11 (d) remain above 0.8 up to the window size of 5 for watermark images and above 0.8 up to the window size of 5 for watermark images with dimensions 256 × 256 and 128 × 128. The NCs in Fig. 11 (e) under Gaussian Noise are all above 0.9 at the variance of 0.001 and degrade to 0.8 up to the variance of 0.007. Moreover, in the sharpening attack (Fig. 11 (f)), the NCs under various strengths are above 0.8.

Safeguarding the image watermark ownership and authentication is one of the applications of invisible watermarking schemes. In this regard, False Positive Problem FPP is becoming a challenging issue in digital invisible watermarking schemes, where an invader states false ownership by

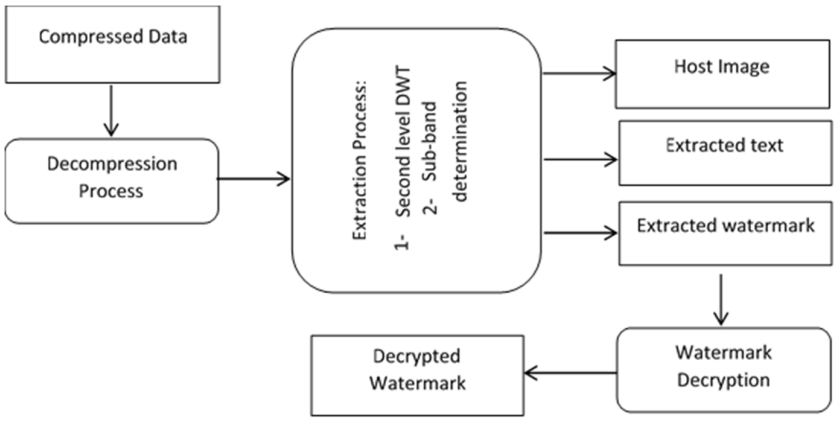

FIGURE 7. Watermark extraction workflow.

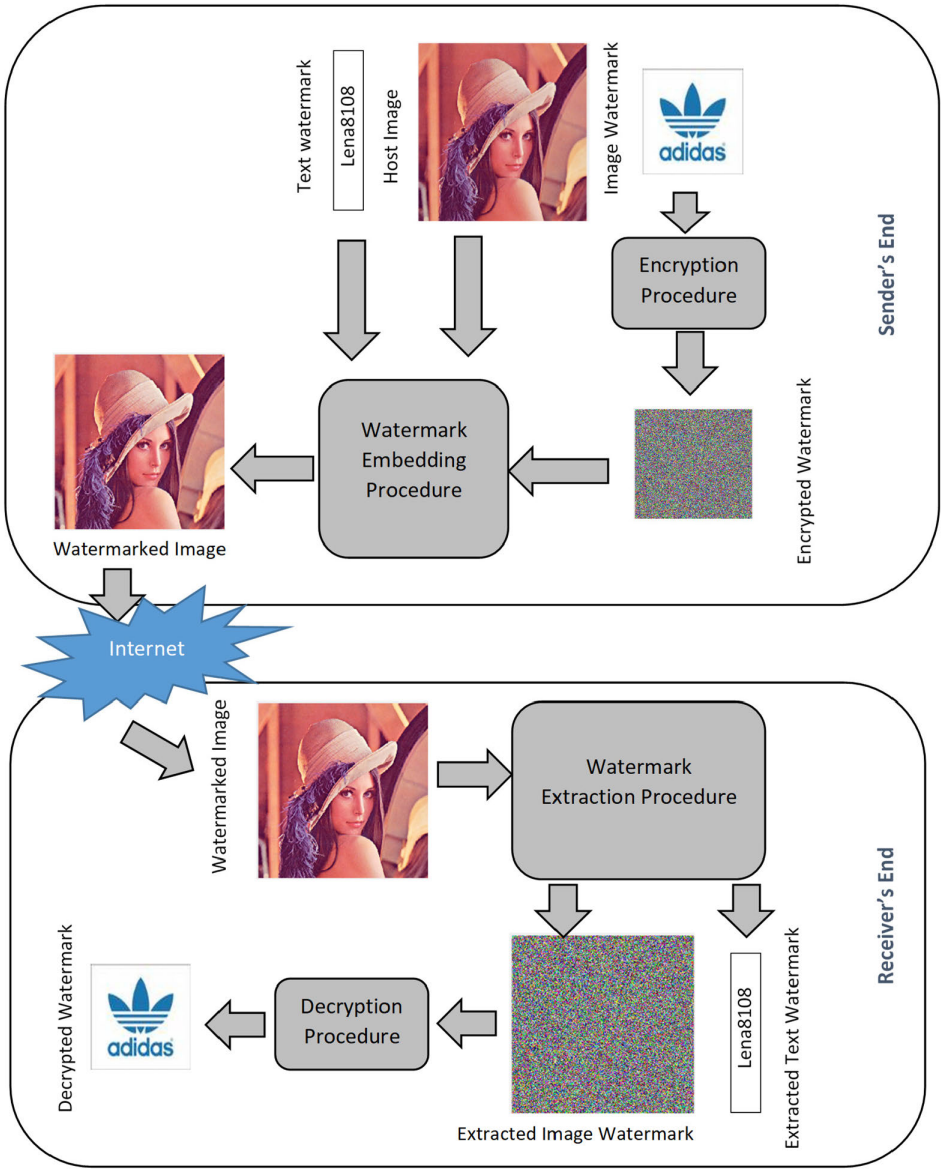

FIGURE 8. An example of the system model.

TABLE 3. Objective measures [3].

Metric	Formula	Description
PSNR	$PSNR(\boldsymbol{C_{img}}, \boldsymbol{WKD_{img}}) = \left(10log_{10}\frac{Pmax^2}{MSE(\boldsymbol{C_{img}}, \boldsymbol{WKD_{img}})}\right)$(5) where $Pmax$ denotes maximum pixel intenTsity in	-Quantifies the similarity between original and watermarked
	an image, and $MSE(\boldsymbol{C_{img}}, \boldsymbol{WKD_{img}}) = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(\boldsymbol{C_{img}}_{i,j} - \boldsymbol{WKD_{img}}_{i,j})^2$	images. -Used for watermark imperceptibility test. -Minimum imperceptibility threshold is 35 db.
NC	$NC(\boldsymbol{W_{img}}, \boldsymbol{XW_{img}}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\boldsymbol{W_{img}}_{i,j}\boldsymbol{EW_{img}}_{i,j}}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\boldsymbol{W_{img}}_{i,j}^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\boldsymbol{EW_{img}}_{i,j}^2}}$. (6)	-It is a quantitative measure of the similarity between the host and extracted watermark image. -Used for robustness test. -Range: [0-1]. - Acceptable above 0.7.
BER	$BER(\boldsymbol{W_{img}}, \boldsymbol{XW_{img}}) = \frac{Eb}{Tb}$(7) where Eb denotes the total number of error bits between the original image watermark and the extracted image watermark, and Tb denotes the total number of watermark bits. Eb can be computed by using Hamming distance.	-Ideally, it should be zero. -Acronym of Bit Error Rate.
SSIM	$SSIM(\boldsymbol{C_{img}}, \boldsymbol{WKD_{img}}) = L(\boldsymbol{C_{img}}, \boldsymbol{WKD_{img}}), C(\boldsymbol{C_{img}}, \boldsymbol{WKD_{img}}), S(\boldsymbol{C_{img}}, \boldsymbol{W}$ (8) where L, C, and S, denote luminance, contrast, and structure comparison functions, respectively.	-It measures the similarity between two images based on luminance, contrast, and structure. -Used for imperceptibility test. -Range: [-1 to +1]. Ideally, it should be +1.
CR	$CR = \frac{S_{ac}}{S_{bc}}$, (9) where S_{ac} and S_{bc} denote the size of data after and before compression respectively .	-0 approaching value is better. -Range: [0-1] -CR value that tends to 0 is considered better.
NPCR and UACI	$NPCR\left(\boldsymbol{EW_{img}}_1, \boldsymbol{EW_{img}}_2\right) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{B(i,j)}{T}$, (10) where $B(i,j)$ denotes bipolar array, T represents the total number of pixels, M, N represent the total number of rows and columns and $B(i,j) = \begin{cases} 0 \ if \ \boldsymbol{EW_{img}}_1(i,j) = \boldsymbol{EW_{img}}_2(i,j) \\ 1 \ if \ \boldsymbol{EW_{img}}_1(i,j) \neq \boldsymbol{EW_{img}}_2(i,j) \end{cases}$, and $UACI\left(\boldsymbol{EW_{img}}_1, \boldsymbol{EW_{img}}_1\right) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left\|\boldsymbol{EW_{img}}_1(i,j) - \boldsymbol{EW_{img}}_2(i,j)\right\|}{F.T}$(11) where F denotes the largest supported pixel.	-NPCR is the Number of Pixel Changing rates, and UACI is the Unified Average Changing Intensity. - Used for differential attack analysis. -higher values of NPCR/ UACI represent higher resistance against differential attacks.

TABLE 3. *(Continued.)* Objective measures [3].

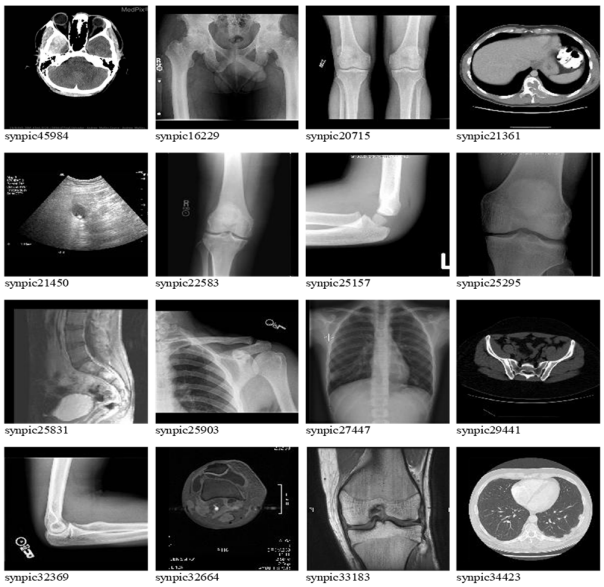

FIGURE 9. Cover images each of dimension (512 × 512) and size [25KB≈27KB].

FIGURE 10. Watermark images, size [2KB≈6KB].

TABLE 4. Performance indicators.

Cover Image	PSNR (db)	SSIM	NC	BER	CR
synpic32664	71.2501	0.997864	0.9992	0	0.8954
synpic32369	70.2303	0.996824	0.9997	0	0.8769
Synpic33183	72.0921	0.998816	0.9965	0	0.8235
Synpic16229	71.2344	0.995981	0.9946	0	0.9025
Synpic20715	70.2432	0.998124	0.9975	0	0.8343
Synpic21361	73.2211	0.997542	0.9969	0	0.8567
synpic45984	72.6265	0.997345	0.9991	0	0.8955
Synpic21450	71.3566	0.996759	0.9986	0	0.8882

inserting and extracting the forged watermarks, thus creating a severe security problem [36]. Specifically, there are two approaches to embedding the watermark by using the SVD domain: Firstly, computing the watermark's and cover

TABLE 5. Average performance computed on hundred images.

Metric	Average value
PSNR	70.3027
SSIM	0.9966
NC	0.9987
BER	0
CR	0.8820
NPCR	0.9951
UACI	0.3459

TABLE 6. Robustness analysis under specific attacks.

Attack	ND-Noise density	NC
SPN -Salt & pepper noise	0.0001 0.0005 0.001	0.893421 0.874461 0.825875
GN- Gaussian noise	0.0001 0.0005	0.879633 0.85246
JC- JPEG compression	QF=10 QF=50 QF=90	0.888452 0.920362 0.977845
Rotation	2^0	0.934102
Speckle noise	0.001	0.925567
Cropping	2%	0.963459
MF- Median filter	[1 1]	0.960473
HE- Histogram equalization		0.864467

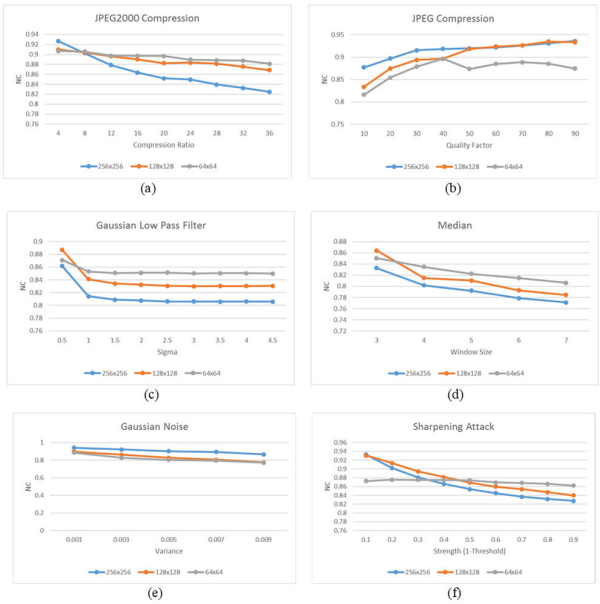

FIGURE 11. NC values between original and extracted watermark under several parameters and attacks: (a) JPEG2000 compression attack, (b) JPEG compression, (c) Gauss low pass filter, (d) Median, (e) Gauss Noise, and (f) Sharpening.

image's singular values and then embedding the image watermark's singular values into the singular values of the cover image. Secondly, embedding the image watermark's bits directly into the singular values of the cover image. But, SVD-based watermarking schemes provide excellent invisibility but come down with an increased probability of FPP. The singular values of the diagonal matrix $\boldsymbol{S}$ are used for embedding the watermark into the host image by using an optimized scaling factor. The SVD components $\boldsymbol{U}$ and $\boldsymbol{V^T}$

TABLE 7. Performance comparison based on average NCs of the proposed scheme under certain attacks.

Attacks	Reference	Reference NC	Proposed (NC)
Gaussian low-pass filter	[56]	0.8476	0.957223
	[57]	0.9951	
	[58]	0.9885	
Median Filtering (5, 1)	[36]	0.9968	0.8914
	[59]	0.5743	
	[60]	0.9356	
	[61]	0.8814	
	[56]	0.8370	
Median Filtering (3, 3)	[62]	0.7897	0.953461
	[63]	0.89	
	[43]	0.9188	
	[58]	0.9994	
	[14]	0.9258	
	[19]	0.5480	
	[64]	0.9929	
Average filter' (3, 3)	[62]	0.7569	0.873236
	[65]	0.9388	
	[64]	0.9684	
Gaussian noise (M=0, V=0.0001)	[36]	0.9706	0.96344
	[59]	0.9256	
	[60]	0.9387	
	[61]	0.9131	
Salt and pepper noise (0.01)	[36]	0.9952	0.942231
	[65]	0.9198	
	Su & Chen, 2017)	0.9287	
	[60]	0.9122	
	[61]	0.9902	
	[66]	0.9421	
Speckle noise (0.005)	[57]	1.0	0.98921
JPEG compression (Qf=30)	[36]	0.9968	0.90232
	[59]	0.8594	
	[65]	0.9198	
	[67]	0.9121	
	[63]	0.887	
	[67]	0.9019	
	[28]	0.9631	
	[60]	0.9789	
JPEG compression (Qf=90)	[43]	0.9862	0.96256
	[66]	0.9061	
	[64]	0.9961	
	[67]	0.9991	
	[44]	0.89109	
Sharpening attack (0.2)	[62]	0.9138	0.97011
	[14]	0.9579	
	[57]	0.9990	
Sharpening attack (1.0)	[36]	0.9638	0.81322
	[59]	0.9877	

TABLE 7. *(Continued.)* **Performance comparison based on average NCs of the proposed scheme under certain attacks.**

	[60]	0.9366	
	[61] c	0.9999	
Histogram equalization	[10]	0.8805	0.85925
	[64]	0.9965	
	[19]	0.5137	
	[28]	0.8456	
Motion blur	[64]	0.9825	0.94294
Flip (Horizontal/Vertical)	[26]	1.0	0.99382

TABLE 8. **Average values of NC, PSNR, and SSIM for comparison without attacks.**

Medical Image Dimensions, Watermark Dimensions	Reference	Reference Value	Proposed Value
512 × 512, 256 × 256	[68])	NC=NA PSNR=72.6763 SSIM=NA	NC=0.99237 PSNR=73.3243 SSIM=0.99891
	[58]	NC=0.99219 PSNR=59.67 SSIM=0.9997	
	[65]	NC=NA PSNR=42.02 SSIM=0.9940	
	[64]	NC=NA PSNR=46.7 SSIM=0.99918	
	[67]	NC=NA PSNR=42 SSIM=0.989	
	[63]	NC=0.9997 PSNR=47.2869 SSIM=0.987	
512 × 512, 64 × 64	[66]	NC=NA PSNR=35.97 SSIM=NA	NC=0.999989 PSNR=76.3451 SSIM=0.99977
	[69]	NC=NA PSNR=38.95 SSIM=NA	
	[44]	NC=NA PSNR=40.77 SSIM=NA	

are used in the extraction process as they provide geometric information. If these components are not encrypted, then it will facilitate the intruder to easily extract the embedded information, consequently causing FPP. Therefore it is necessary to encrypt these components to avoid the FPP [11]. Hence, encryption of these components, i.e., $\boldsymbol{U}$ and $\boldsymbol{V^T}$ serves as an additional layer of security against FPPs.

Therefore, we have exploited double-layer encryption to cope with the FPP problem. The first layer makes use of the higher dimensional chaotic system that encrypts the watermark image, whereas the second layer encrypts the SVD components i.e. $\boldsymbol{U_{LH1}}$ and $(\boldsymbol{V_{LH1}})^{\boldsymbol{T}}$ By using the logistic map, thereby providing extra security against FPP, that is, an intruder with forged $\boldsymbol{U_{LH1}}$ and $(\boldsymbol{V_{LH1}})^{\boldsymbol{T}}$ components would only extract the insignificant watermarks.

TABLE 9. **Average computational time comparison. The cover images of figure 9 and watermark images of figure 10 are used to compute the average values.**

Average Computational Time (s)	Reference	Reference Value	Proposed
Watermark Embedding Time	[62]	0.8509	0.28634
	[43]	0.611810	
	[67]	0.1419	
	[70]	1.96	
	[65]	2.2776 (By using Robust Algorithm)	
	[56]	0.7901	
Watermark Encryption Time	[65]	0.8736 (By using Chaotic + DNA Encryption)	0.947
Compression Time	[56]	0.2015	0.2143
Overall Average Time (s)	[63]	2.1	1.44764
	[71]	1.3514	
	[72]	1.9915	

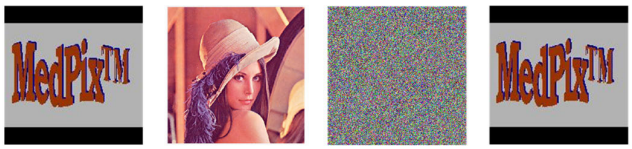

FIGURE 12. **FPP simulation: (a) original watermark, (b) watermarked image, (c) watermark extracted from the watermarked image with incorrect parameters, which is random like and is not recognizable, and (d) watermark extracted from the watermarked image with correct parameters which is not random like and is recognizable.**

Therefore, the components of the watermark image U and VT of SVD are encrypted to solve this problem in this work; that is, an attacker with counterfeit U and VT could only extract a random-like watermark.

A watermark (64 × 64) is chosen to simulate the FPP, as shown in Fig. 12 (a). The watermark is first encrypted and embedded into the cover image Lena (512 × 512). Fig. 12 (b) is the watermark extracted from the watermarked image with incorrect parameters, which is random and unfamiliar; Fig. 12 (c) is the watermark extracted from the watermarked image with incorrect parameters, which is random and unfamiliar, Fig. 12 (d) is the watermark extracted from the watermarked image with correct parameters which is not random like and is familiar.

VI. CONCLUSION AND FUTURE WORK

This article proposed a blind watermarking scheme based on three modules, generator, protector, and resizer, to deal with the issues such as image authentication, detachment

avoidance between the watermark and its corresponding host image, and confidentiality of watermarks in the host image. Watermarks of various dimensions can be embedded into the host image. Average PSNRs without attacks of watermarked images exceed 70db. And average PSNRs of extracted watermarks under specific attacks remain in the range [28-40db]. Similarly, average NCs under specific attacks listed in Table 6 are all greater than 0.85 for Gaussian low pass filter, Median filtering, Average filtering, and Histogram Equalization and more significant than 0.9 for Gaussian Noise, Salt & Pepper Noise, JPEG Compression, and Flip horizontal/ vertical attack. Anyway, the proposed scheme has demonstrated exemplary performance towards imperceptibility, security, robustness, and compression ratio.

In the future, we aim to substitute the proposed scheme with other transformations, encryption, and compression techniques to make it capable of administering DICOM imaging formats. Moreover, the concept of deep learning with better error-correcting codes can be integrated to make it more secure and robust.

Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] H. Aljuaid and S. A. Parah, "Secure patient data transfer using information embedding and hyperchaos," *Sensors*, vol. 21, no. 1, pp. 1–20, 2021.
[2] A. K. Singh, B. Kumar, G. Singh, and A. Mohan, *Medical Image Watermarking: Techniques and Applications*. Cham, Switzerland: Springer, 2017.
[3] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Comput. Commun.*, vol. 152, pp. 72–80, Feb. 2020.
[4] X. Li, S.-T. Kim, and I.-K. Lee, "Robustness enhancement for image hiding algorithm in cellular automata domain," *Opt. Commun.*, vol. 356, no. 1, pp. 186–194, 2015.
[5] Q. Su, Y. Niu, H. Zou, Y. Zhao, and T. Yao, "A blind double color image watermarking algorithm based on QR decomposition," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 987–1009, 2014.
[6] J. M. Carracedo, M. Milliken, P. K. Chouhan, B. Scotney, Z. Lin, A. Sajjad, and M. Shackleton, "Cryptography for security in IoT," in *Proc. 5th Int. Conf. Internet Things, Syst., Manage. Secur.*, 2018, pp. 23–30.
[7] H. Nazir, I. S. Bajwa, M. Samiullah, W. Anwar, and M. Moosa, "Robust secure color image watermarking using 4D hyperchaotic system, DWT, HbD, and SVD based on improved FOA algorithm," *Secur. Commun. Netw.*, vol. 2021, Jun. 2021, Art. no. 6617944.
[8] R. Schmitz, "Use of SHDM in commutative watermarking encryption," *EURASIP J. Inf. Secur.*, vol. 2021, no. 1, 2021, doi: 10.1186/s13635-020-00115-w.
[9] C.-C. Chang, C.-T. Li, and Y.-Q. Shi, "Privacy-aware reversible watermarking in cloud computing environments," *IEEE Access*, vol. 6, pp. 70720–70733, 2018.
[10] T. K. Araghi, A. A. Manaf, and S. K. Araghi, "A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition," *Expert Syst. Appl.*, vol. 112, pp. 208–228, Dec. 2018.
[11] J. Liu, J. Huang, Y. Luo, L. Cao, S. Yang, D. Wei, and R. Zhou, "An optimized image watermarking method based on HD and SVD in DWT domain," *IEEE Access*, vol. 7, pp. 80849–80860, 2019.
[12] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," *Information*, vol. 11, no. 2, pp. 1–38, 2020.
[13] H. Singh, "Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain," *IET Image Process.*, vol. 12, no. 11, pp. 1994–2001, 2018.
[14] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption," *IEEE Access*, vol. 6, pp. 19876–19897, 2018.
[15] S. Wang, D. Guo, X. Xu, L. Zhuo, and M. Wang, "Cross-modality retrieval by joint correlation learning," *ACM Trans. Multimedia Comput., Commun. Appl.*, vol. 15, no. 2s, pp. 1–16, 2019.
[16] T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD," *Future Gener. Comput. Syst.*, vol. 101, pp. 1223–1246, Dec. 2019.
[17] Y. Shen, C. Tang, M. Xu, M. Chen, and Z. Lei, "A DWT-SVD based adaptive color multi-watermarking scheme for copyright protection using AMEF and PSO-GWO," *Expert Syst. Appl.*, vol. 168, Apr. 2021, Art. no. 114414.
[18] J.-M. Guo, D. Riyono, and H. Prasetyo, "Hyperchaos permutation on false-positive-free SVD-based image watermarking," *Multimedia Tools Appl.*, vol. 78, no. 20, pp. 29229–29270, Oct. 2019.
[19] N. Singh, S. Joshi, and S. Birla, "Color image watermarking with watermark authentication against false positive detection using SVD," in *Proc. Int. Conf. Sustain. Comput. Sci.*, 2019, pp. 399–405.
[20] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 26845–26879, Oct. 2018.
[21] K. Zhan and W. Jiang, "Novel four-wing hyper-chaos system and its application in image encryption," *Comput. Eng. Appl.*, vol. 53, no. 12, pp. 36–44, 2017.
[22] P. Aparna and P. V. V. Kishore, "Biometric-based efficient medical image watermarking in E-healthcare application," *IET Image Process.*, vol. 13, no. 3, pp. 421–428, 2019.
[23] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.
[24] M. Rüdisüli, T. J. Schildhauer, S. M. A. Biollaz, and J. R. Van Ommen, "Measurement, monitoring and control of fluidized bed combustion and gasification," in *Fluidized Bed Technologies for Near-Zero Emission Combustion and Gasification*. Philadelphia, PA, USA: Woodhead Publishing, 2013.
[25] C.-C. Chen and C.-C. Chang, "High-capacity reversible data-hiding for LZW codes," in *Proc. 2nd Int. Conf. Comput. Modeling Simulation*, Jan. 2010, pp. 3–8.
[26] B. Hassan, R. Ahmed, B. Li, and O. Hassan, "An imperceptible medical image watermarking framework for automated diagnosis of retinal pathologies in an eHealth arrangement," *IEEE Access*, vol. 7, pp. 69758–69775, 2019.
[27] Y.-M. Li, D. Wei, and L. Zhang, "Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain," *Inf. Sci.*, vol. 551, pp. 205–227, Apr. 2021.
[28] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, "A lossless DWT-SVD domain watermarking for medical information security," *Multimedia Tools Appl.*, vol. 80, no. 16, pp. 24823–24841, Jul. 2021.
[29] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Sci. Int.*, vol. 320, Mar. 2021, Art. no. 110691.
[30] R. Singh and A. Ashok, "An optimized robust watermarking technique using CKGSA in frequency domain," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102734.
[31] M. Zhang, W. Ding, Y. Li, J. Sun, and Z. Liu, "Color image watermarking based on a fast structure-preserving algorithm of quaternion singular value decomposition," *Signal Process.*, vol. 208, Jul. 2023, Art. no. 108971.
[32] M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Image watermarking using separable fractional moments of Charlier–Meixner," *J. Franklin Inst.*, vol. 358, no. 4, pp. 2535–2560, Mar. 2021.
[33] M. Sadeghi, R. Toosi, and M. A. Akhaee, "Blind gain invariant image watermarking using random projection approach," *Signal Process.*, vol. 163, pp. 213–224, Oct. 2019.
[34] M. Cedillo-Hernandez, A. Cedillo-Hernandez, M. Nakano-Miyatake, and H. Perez-Meana, "Improving the management of medical imaging by using robust and secure dual watermarking," *Biomed. Signal Process. Control*, vol. 56, Feb. 2020, Art. no. 101695.
[35] H.-T. Hu, L.-Y. Hsu, and H.-H. Chou, "An improved SVD-based blind color image watermarking algorithm with mixed modulation incorporated," *Inf. Sci.*, vol. 519, pp. 161–182, May 2020.
[36] 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," *Appl. Soft Comput. J.*, vol. 84, pp. 1–30, Jan. 2019.

[37] N. R. Zhou, A. W. Luo, and W. P. Zou, "Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 2507–2523, Jan. 2019.
[38] M. Sundararajan and G. Yamuna, "Optimization of colour image watermarking using area of best fit equation and Cuckoo search algorithm," *Mater. Today, Proc.*, vol. 5, no. 1, pp. 1138–1146, 2018.
[39] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm," *Expert Syst. Appl.*, vol. 41, no. 17, pp. 7858–7867, 2014.
[40] I. A. Ansari, M. Pant, and C. W. Ahn, "Artificial bee colony optimized robust-reversible image watermarking," *Multimedia Tools Appl.*, vol. 76, no. 17, pp. 18001–18025, Sep. 2017.
[41] B. Wang, "An adaptive image watermarking method combining SVD and Wang–Landau sampling in DWT domain," *Mathematics*, vol. 8, pp. 1–20, Jan. 2020.
[42] X. Cui, Y. Niu, X. Zheng, and Y. Han, "An optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image," *PLoS ONE*, vol. 13, no. 5, pp. 1–15, 2018.
[43] M. Y. Valandar, M. J. Barani, and P. Ayubi, "A blind and robust color images watermarking method based on block transform and secured by modified 3-dimensional Hénon map," *Soft Comput.*, vol. 24, no. 2, pp. 771–794, Jan. 2020.
[44] K. Fares, K. Amine, and E. Salah, "A robust blind color image watermarking based on Fourier transform domain," *Optik*, vol. 208, no. March, pp. 1–9, 2020.
[45] K. Hao, G. Feng, and X. Zhang, "Robust image watermarking based on generative adversarial network," *China Commun.*, vol. 17, no. 11, pp. 131–140, Nov. 2020.
[46] A. A. R. Alkhafaji, N. N. A. Sjarif, M. A. Shahidan, N. F. M. Azmi, H. M. Sarkan, S. Chuprat, O. I. Khalaf, and E. N. Al-Khanak, "Payload capacity scheme for Quran text watermarking based on vowels with Kashida," *Comput., Mater. Continua*, vol. 67, no. 3, pp. 3865–3885, 2021.
[47] C.-Y. Yang and W.-F. Wang, "An efficient data hiding for ECG signals based on the integer wavelet transform and block standard deviation," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5868–5882, Sep. 2022.
[48] K. Fares, A. Khaldi, K. Redouane, and E. Salah, "Biomedical signal processing and control DCT & DWT based watermarking scheme for medical information security," *Biomed. Signal Process. Control*, vol. 66, Jan. 2021, Art. no. 102403.
[49] M. S. Moad, M. R. Kafi, and A. Khaldi, "A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications," *Microprocessors Microsystems*, vol. 90, Apr. 2022, Art. no. 104490.
[50] T. Li, K. Liu, W. Feng, C. Yang, and X. Luo, "HeteroTiC: A robust network flow watermarking based on heterogeneous time channels," *Comput. Netw.*, vol. 219, Dec. 2022, Art. no. 109424.
[51] M. Tang and F. Zhou, "A robust and secure watermarking algorithm based on DWT and SVD in the fractional order Fourier transform domain," *Array*, vol. 15, Sep. 2022, Art. no. 100230.
[52] E. Akhtarkavan, B. Majidi, and A. Mandegari, "Secure medical image communication using fragile data hiding based on discrete wavelet transform and A_5 lattice vector quantization," *IEEE Access*, vol. 11, pp. 9701–9715, 2023.
[53] E. Hasanzadeh and M. Yaghoobi, "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7279–7297, 2019.
[54] A. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, Tech. Rep. SP 800-22 Rev. 1a, Accessed: Apr. 2, 2010. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf
[55] W. H. Alshoura, Z. Zainol, J. S. Teh, M. Alawida, and A. Alabdulatif, "Hybrid SVD-based image watermarking schemes: A review," *IEEE Access*, vol. 9, pp. 32931–32968, 2021.
[56] K. Prabha and I. Shatheesh Sam, "An effective robust and imperceptible blind color image watermarking using WHT," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 10, p. 11, Jan. 2020.
[57] D. Ariatmanto and F. Ernawan, "An improved robust image watermarking by using different embedding strengths," *Multimedia Tools Appl.*, vol. 79, nos. 17–18, pp. 12041–12067, 2020.
[58] A. Bose and S. P. Maity, "Journal of information security and applications secure sparse watermarking on DWT-SVD for digital images," *J. Inf. Secur. Appl.*, vol. 68, no. July, Art. ID:103255, 2022.
[59] Q. Su and B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft Comput.*, vol. 22, no. 1, pp. 91–106, Jan. 2018.
[60] S. Roy and A. K. Pal, "An SVD based location specific robust color image watermarking scheme using RDWT and Arnold scrambling," *Wireless Pers. Commun.*, vol. 98, no. 2, pp. 2223–2250, Jan. 2018.
[61] Q. Su, G. Wang, X. Zhang, G. Lv, and B. Chen, "A new algorithm of blind color image watermarking based on LU decomposition," *Multidimensional Syst. Signal Process.*, vol. 29, no. 3, pp. 1055–1074, Jul. 2018.
[62] H. Zhang and C. Wang, "A robust image watermarking scheme based on SVD in the spatial domain," *Future Internet*, vol. 9, no. 45, pp. 1–16, 2017.
[63] H. M. Al-Otum and A. A. A. Ellubani, "Secure and effective color image tampering detection and self restoration using a dual watermarking approach," *Optik*, vol. 262, Jul. 2022, Art. no. 169280.
[64] Y. Luo, L. Li, J. Liu, S. Tang, L. Cao, S. Zhang, S. Qiu, and Y. Cao, "A multi-scale image watermarking based on integer wavelet transform and singular value decomposition," *Expert Syst. Appl.*, vol. 168, Apr. 2021, Art. no. 114272.
[65] A. Kamili, N. N. Hurrah, S. A. Parah, G. M. Bhat, and K. Muhammad, "DWFCAT: Dual watermarking framework for industrial image authentication and tamper localization," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5108–5117, Jul. 2021.
[66] Y. Cao, F. Yu, and Y. Tang, "A digital watermarking encryption technique based on FPGA cloud accelerator," *IEEE Access*, vol. 8, pp. 1–15, 2020.
[67] H. Cao, F. Hu, Y. Sun, S. Chen, and Q. Su, "Robust and reversible color image watermarking based on DFT in the spatial domain," *Optik*, vol. 262, Jul. 2022, Art. no. 169319.
[68] N. Jayashree and R. S. Bhuvaneswaran, "A robust image watermarking scheme using Z-transform, discrete wavelet transform and bidiagonal singular value decomposition," *Comput., Mater. Continua*, vol. 58, no. 1, pp. 263–285, 2019.
[69] H. Xu, X. Kang, Y. Chen, and Y. Wang, "Rotation and scale invariant image watermarking based on polar harmonic transforms," *Optik*, vol. 183, pp. 401–414, Apr. 2019.
[70] H. M. Al-Otum and M. Ibrahim, "Color image watermarking for content authentication and self-restoration applications based on a dual-domain approach," *Multimedia Tools Appl.*, vol. 80, no. 8, pp. 11739–11764, Mar. 2021.
[71] R. Wang, H. Shaocheng, P. Zhang, M. Yue, Z. Cheng, and Y. Zhang, "A novel zero-watermarking scheme based on variable parameter chaotic mapping in NSPD-DCT domain," *IEEE Access*, vol. 8, pp. 182391–182411, 2020.
[72] D. Liu, Q. Su, Z. Yuan, and X. Zhang, "A blind color digital image watermarking method based on image correction and eigenvalue decomposition," *Signal Process., Image Commun.*, vol. 95, Jul. 2021, Art. no. 116292.

HIRA NAZIR received the B.S. degree in information technology, the M.S. degree in software engineering, and the Ph.D. degree in computer science from The Islamia University of Bahawalpur, Pakistan. She is currently an Assistant Professor with the Department of Computer Science, Muhammad Nawaz Sharif University of Agriculture, Multan, Pakistan. Her research interests include formal methods, process models in software engineering, digital image watermarking, social network data analysis, and information security.

MUHAMMAD SAMI ULLAH received the B.S. degree in computer science, the M.B.A. degree in marketing, and the M.S. and Ph.D. degrees in computer science from The Islamia University of Bahawalpur, Pakistan. He is currently a Visiting Faculty Member with Muhammad Nawaz Shareef University, Multan, as well as Permanent Faculty Member at the Government Sadiq Graduate College of Commerce, Bahawalpur. Government Sadiq Graduate College of Commerce, Bahawalpur. His research interests include wireless network virtualization, radio resource allocation, interference management for cellular systems and applications of nonlinear dynamics, and DNA computing in information security.

SYED SALMAN QADRI received the Ph.D. degree from The Islamia University of Bahawalpur, Pakistan. He is currently working as an Associate Professor and the Chairperson of the Department of Computer Science, Muhammad Nawaz Sharif University of Agriculture, Multan, Pakistan. His research interests include software testing, Agile, the IoT, cloud computing, sliding mode control, fractional control, neural networks, cognitive radio networks, and network security.

HUMAIRA ARSHAD is currently an Associate Professor and the Chairperson of the Department of Computer Science, The Islamia University of Bahawalpur, Pakistan. Her research interests include wireless sensor networks, the Internet of Things (IoT), scheduling patterns of sensor messages, node failure management, and QoS-aware message scheduling.

MUJTABA HUSNAIN is currently an Associate Professor with the Department of Information Technology, The Islamia University of Bahawalpur, Pakistan. His research interests include machine learning, artificial intelligence, data visualization, algorithm analysis, and graph theory.

ABDUL RAZZAQ received the Ph.D. degree in computer science from China. He is currently an Associate Professor and the Director of information technology with the Muhammad Nawaz Sharif University of Agriculture, Multan Pakistan. His research interests include data mining and natural language processing.

SYED ALI NAWAZ received the Ph.D. degree in computer science from The Islamia University of Bahawalpur, Pakistan. He is currently an Assistant Professor with the Department of Information Technology, The Islamia University of Bahawalpur. His research interests include computer communications (networks), data mining, and natural language processing.