Multimedia Tools and Applications
https://doi.org/10.1007/s11042-020-09941-z

Multi-level security of medical images based on encryption and watermarking for telemedicine applications

Rohit Thanki[1] · Ashish Kothari[2]

Received: 30 April 2019 / Revised: 14 September 2020 / Accepted: 17 September 2020
Published online: 28 September 2020

Abstract

In this paper, a robust and hybrid domain watermarking scheme is proposed for the security of medical images in telemedicine applications. The secret identity of the patient is inserting into the cover medical image using the hybridization of ridgelet transform and singular value decomposition for the purposed of identification and authentication. For better security of watermarked medical image, the Arnold scrambling based encryption is applying to it before sending it at the receiver end. The main advantage of this scheme is multi-level security where secret patient information is inserted to cover medical image to get a secure watermarked medical image using watermarking. Then, encryption is applied to the watermarked medical image to generate its encrypted version. Thus, this proposed scheme provides multi-level security using watermarking and encryption. The advantage of multi-level security in the proposed scheme is that if an imposter or attacker tries to get patient identity from the medical image, he or she requires multiple information in terms of extraction steps and keys, etc. The other reason for proposed this scheme that it improves the payload capacity of many existing watermarking schemes. Experimental results of the scheme indicated that the proposed scheme provides high imperceptibility and more robustness against various types of attacks. Further, the performance of the proposed scheme is found better than existing medical watermarking schemes. Furthermore, quality checking of watermarked medical image is done by various quality measures which are indicated that the quality of the image has fulfilled the benefits of secure telemedicine applications.

Keywords Arnold · Finite ridge transform (FRT) · Medical image · Singular value decomposition (SVD) · Telemedicine · Watermarking

✉ Rohit Thanki
rohitthanki9@gmail.com

[1] R & D Head, Prognica Labs, Dubai, United Arab Emirates

[2] Atmiya University, Rajkot, India

1 Introduction

In today's E-era that mainly includes E-commerce, E-banking, E-health, and E-learning, information can be effectively downloaded with no authorization from the proprietor. Once in a while, these circumstances make different issues, for example, copyright security and proprietor verification. In such cases, assurance and verification of advanced information are required before it is exchanged over an open-source transmission medium. To answer these issues, analysts proposed different information concealing strategies: cryptography, steganography, and watermarking [5, 31]. Watermarking is primarily utilized for the assurance and validation of information. This method beats the constraints of steganography by embedding a watermark into host content such that even the basic client cannot find out the hidden watermark. As per literature [2, 4, 5, 25, 31], the watermarking framework has three components: a watermark embedder, a correspondence channel that might be wired or wireless, and a watermark extractor. The watermark embedder embeds a watermark into host images to generate a watermarked image, while watermark extractor extracts the watermark from the test image which can be the watermarked image with or without attacks. Major requirements of digital image watermarking are recalled here [2, 4, 5, 25, 31]:

a. **Robustness:** The watermarking scheme must protect owners' data against any manipulations and has to be robust.
b. **Imperceptibility:** After the watermark insertion into host data, the visual quality of the host data should not be affected much, i.e., the watermark should be imperceptible.
c. **Embedding Capacity:** The watermarking scheme should allow hiding large size watermarks [4].

The watermarking schemes are majorly developed in three processing domains: spatial domain, transform domain, and hybrid domain [22, 31]. The spatial domain schemes are easy to implement but provide less imperceptibility as the host image pixels are directly modified. The transform domain watermarking is complex but provides more robustness compared to the spatial domain watermarking. In all the transform domain schemes, the host image is converted into the frequency domain using various image transforms such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) [12, 15], Discrete Wavelet Transform (DWT) before watermark embedding and is inverse transformed later. In all the hybrid domain schemes, the host image is converted into the hybrid coefficients of frequency using various image transforms before watermark embedding and is inverse transformed later. Recently, new transforms such as Fast Discrete Curvelet Transform (FDCuT) [32], Non-subsampled Contourlet Transform (NSCT) [23], and Finite Ridgelet Transform (FRT) [28] based watermarking schemes are proposed by various researchers. Out of these, all transforms, the mid frequency DCT weights of the cover image are widely used for the embedding of watermark image in most of the watermarking schemes. The reason behind the usage of these weights that it provides more robustness compared to other weights against watermarking attacks.

The main challenges of designing of watermarking schemes for the security of medical image are following as [2, 4, 5, 22, 25, 31]: (a) it should be blind or non-blind (b) it should be robust against various watermarking attacks (c) it should provide hide or embed more patient or owner identification into the cover medical image. The watermarking schemes are mainly used for the security of medical image in telemedicine applications where medical image transfers from one hospital or remote health care center to another hospital or remote health care. Therefore, in this paper, a new watermarking scheme is a design based on finite ridgelet transform (FRT), singular value decomposition (SVD), and Arnold scrambling based encryption which provides robustness against watermarking attacks and embeds more patient or owner identification.

The rest of the paper is organized as follows. The summary of some recently published research work related to proposed work is discussed in section 2. The main contribution of the proposed work is discussed in section 3. Section 4 discussed the proposed embedding and extraction process. In section 5, the experimental results of the proposed work are briefly discussed. Finally, the concluding points of the paper are given in section 6.

2 Related work

In this section, some important research work in the area of medical image security is presented. Recently, many researchers were reported watermarking schemes for the security of the medical image [30]. Arunkumar et al. [1] proposed a nonblind and hybrid domain medical image watermarking scheme based on discrete cosine transform (DCT), redundant integer wavelet transform (RIWT) and singular value decomposition (SVD). In this scheme, the patient information is inserted into the hybrid coefficients of the medical image using additive watermarking. Experimental results show that this scheme has good imperceptibility and robustness. A watermarking scheme with encryption for the security of medical images is proposed in [20]. This scheme is based on IWT and the least significant bit (LSB) substitution. In [19], a model for security of medical image in telemedicine applications is proposed.

A multi-layer watermarking scheme based on the hybridization of DWT, DCT, SVD and chaotic encryption is proposed in [27]. In this scheme, the watermarked medical image is encoded by chaotic encryption after inserting watermark information into it. A quartic digital signature-based medical image authentication scheme is proposed in [3]. A robust watermarking scheme based on DCT and DWT is proposed in [26]. In this scheme, first, the medical image is divided into two parts such as the region of interest (ROI) and the region of non-interest (RONI). Then, the watermark is inserted into hybrid coefficients of RONI of the medical image.

A robust and multiple-layer watermarking scheme based on non-subsampled contourlet (NSCT), redundant discrete wavelet transform (RDWT), SVD, and chaotic encryption is proposed in [26]. In this scheme, three encrypted watermark information is inserted into the medical image for security in telemedicine applications. A fragile watermarking scheme based on NSCT and Compressive Sensing (CS) based encryption for authentication of the medical image was introduced in [29]. A watermarking scheme based on DCT and CS based encryption for tamper detection in the medical image was introduced in [6].

3 Main contribution of the proposed work

This paper presents a non-blind and robust watermarking scheme for the secure medical image which is based on a combination of finite ridgelet transform (FRT), singular value decomposition (SVD), and Arnold scrambling based encryption. The reason behind choosing SVD in this scheme is that it is performed faster than random projections based on noise sequence [13, 14, 18] which was used in the scheme reported in [32]. The FRT and SVD are very popular transform and very well discussed in [7]. Arnold scrambling [16, 21] is an image encryption scheme which is based on a chaotic map and it's applied to a watermarked medical image to provide security to the medical image before sending it to the receiver side. Therefore, this proposed scheme provides multiple levels of security to the medical image by using watermarking and encryption. Also, the size of patient information is double than the size of cover medical image and this information hides into a cover medical image using the proposed scheme. This step improves the payload capacity of traditional watermarking schemes which were reported in [1, 20, 26, 27]. These two are major contributions of this proposed scheme. The other minor contributions of the proposed scheme are as follows:

- **Security of Owner Identity:** The security of patient identity is maintained because it is inserted into the medical image.
- **Improved Security:** In the proposed scheme, the watermarked medical image is encrypted after the watermark is inserted into it. The performance of the encryption scheme measures using NPCR and UACI. The evaluation of an encryption scheme indicated that this scheme improves security in the scheme without affecting the performance of it.
- **Improved Imperceptibility:** The imperceptibility of some existing medical watermarking schemes [26, 27] is very less which overcomes by the proposed scheme. The imperceptibility of watermarking scheme is measured using quality parameter like Peak Signal to Noise Ratio (PSNR) (which was measured in decibels (dB)) and the value of this parameter in existing schemes [26, 27] is varying around 20 dB to 40 dB while in proposed scheme, the value of this parameter is achieved in range of 35 dB to 59 dB. This is indicated that this proposed scheme provide better imperceptibility compared to existing schemes [26, 27] in the literature.

4 Proposed scheme

The proposed scheme develops based on the hybridization of FRT and SVD along with Arnold scrambling. This scheme is non-blind and robust. The main reason for using FRT is that it decomposed image into its double size, i.e. if an image has a size of $M \times N$ then it sizes of ridgelet transform coefficients is $2\ M \times 2\ N$. Thus, the size of the $2\ M \times 2\ N$ size of the watermark image can be embedded into the size of $M \times N$ of the cover image which improves the payload capacity of the watermarking scheme. The SVD is used in the proposed scheme to provides robustness against any watermarking attacks such as the addition of noise, filtering, compression, etc. While Arnold scrambling is used for security of watermarked medical image before transmission on an open communication channel. The reason behind using Arnold scrambling in the proposed scheme is that it is easy to implement and fast computational time compared to other encryption algorithms such as DES, AES, etc. Thus, the combination of FRT and SVD along with Arnold scrambling based encryption in the proposed scheme is used to achieved high payload capacity, more robustness, and security of medical images when it transfers from one place to another place.

In this proposed scheme, the medical image is converted into its transform domain using the hybridization of FRT and SVD. However, the watermark image is converted into its transform domain using SVD. Finally, the singular value of the medical image is modifying by the singular value of the watermark image to get the watermarked medical image. Further, the watermarked medical image is encrypted using Arnold scrambling based on the secret key to get encrypted watermarked medical images. The extraction of the watermark image is followed by reverse steps of the watermark embedding process. The complete process of the proposed scheme is shown in Fig. 1 (a & b).

4.1 Embedding process

The watermark image can be embedded in to cover medical image using the following steps:

Step 1: Take the cover medical image (***MI***) and watermark image (***W***) for further process.
Step 2: Apply 1st level forward finite ridgelet transform (FRT) to the cover medical image to get its ridgelet to transform coefficients (**FRT(MI) → FRm**).
Step 3: Apply forward singular value decomposition (SVD) to the ridgelet transform coefficients of a cover medical image to get its hybrid to transform coefficients (**SVD(FRm) → Um, Sm, Vm**).

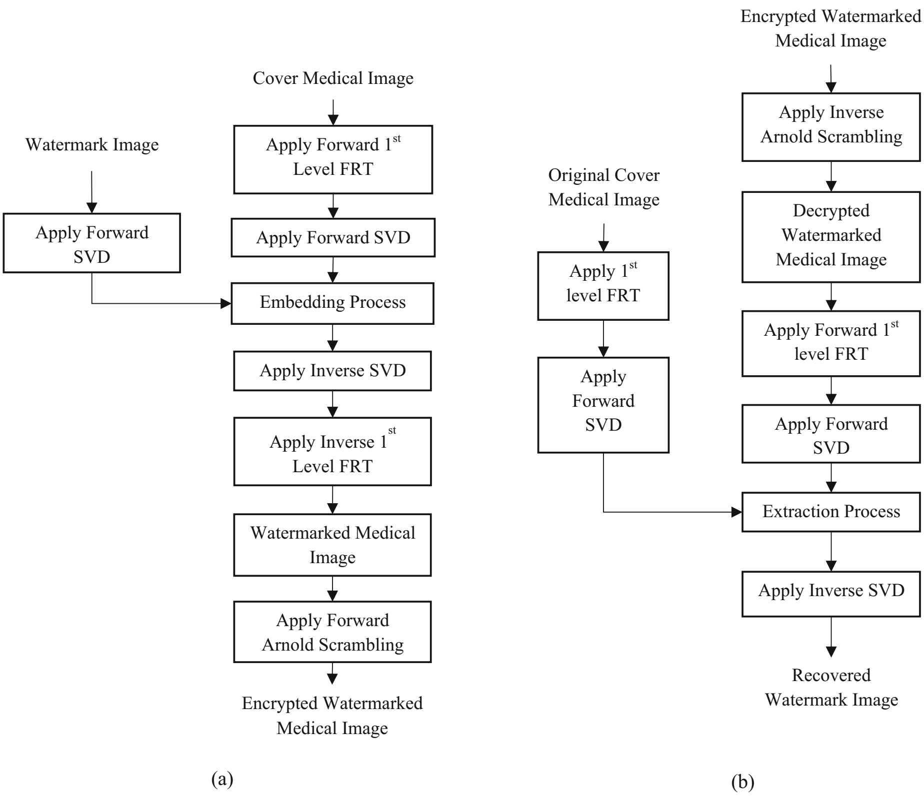


Fig. 1 Block Diagram of Proposed Scheme (a) Embedding Process (b) Extraction Process

Step 4: Apply forward singular value decomposition to watermark image (***W***) to get its singular value (**SVD (W) → Sw**).

Step 5: Then, the singular value of the watermark image (***Sw***) is inserted into the hybrid transform coefficients of cover medical image (***Sm***) using the additive watermarking equation:

$$MSm = Sm + \alpha \times Sw \tag{1}$$

Step 6: Apply inverse SVD on modified singular value (***MSm***) to get modified ridgelet coefficients of cover medical image (***IFRm***) (**IFRm → Um × MSm × Vm′**).

Step 7: Apply 1st level inverse FRT on modified ridgelet coefficients of cover medical image (***IFRm***) to get the watermarked medical image (**IFRT(IFRm) → WMI**.)

Step 8: Finally, forward Arnold scrambling is applied to the watermarked medical image (***WMI***) using a secret key (***k***) to obtain an encrypted watermarked medical image (***EWMI***).

4.2 Extraction process

The watermark image can be extracted from the encrypted watermarked medical image using the following steps:

Step 1: An inverse Arnold scrambling is applied to the encrypted watermarked medical image, (***EWMI***) using a secret key (***k***) to obtain a decrypted watermarked medical image (***DWMI***).

Step 2: Apply 1st level forward FRT on the decrypted watermarked medical image to ridgelet transform coefficients of it (**FRT(DWMI) → DFRm**).

Step 3: Apply forward SVD on ridgelet transform coefficients of decrypted watermarked medical image (***DFRm***) to get its singular value (**SVD(DFRm) → DUm, DSm, DVm′**).

Step 4: The singular value of the watermark image (***ESw***) is extracted from the decrypted watermarked medical image using the below equation:

$$ESw = (DSm - Sm)/\alpha \tag{2}$$

Step 5: Apply inverse SVD on the extracted singular value of watermark image (***ESw***) to get recovered watermark image (***EW***) (**EW → Uw × ESw × Vw′**).

5 Experimental results and discussion

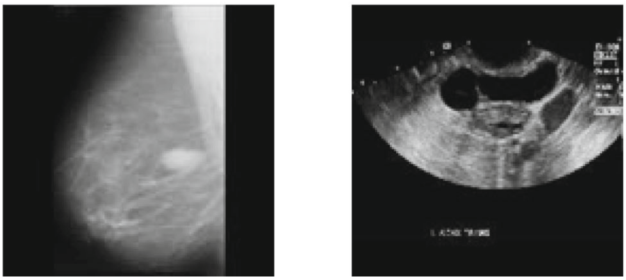
In this section, the simulation results of the proposed scheme using various types of medical images and watermark information. This section divides into various subsections such as information of test images and Quality Measures, results about imperceptibility, and robustness of the proposed scheme. Finally, the results of the proposed scheme are compared with the results of existing schemes with various parameters.

5.1 Information on test images and quality measures

The testing and analysis of the proposed scheme are done using various types of cover medical images such as CT, MRI, US, X-ray, and mammography. These images are obtained from various public medical databases [17, 24] and the size of the images is 128 × 128 pixels with 8-bit grayscale (shown in Fig. 2). The various owner information in terms of watermark images such as binary logo and sample patient information is used for the experiment (shown in Fig. 3). The size of the watermark image is 256 × 256 pixels.

The performance of the proposed scheme is evaluated using various quality measures such as peak signal to noise ratio (PSNR) [11, 32] and normalized correlation (NC) [11, 32]. The PSNR is measured in terms of decibels (dB), used to measure the imperceptibility of the watermark into cover medical image and is calculated using eq. (3):

(a) (b) (c)



(d) (e)

Fig. 2 Test Cover Medical Images (a) Body CT (b) Neck X-ray (c) Brain MRI (d) Breast Mammography (e) US

(a) (b)

Fig. 3 Test Watermark Images (a) Binary Logo (b) Sample Patient Information

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \tag{3}$$

$$MSE = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(CMI(i,j) - WMI\left(i,j\right)\right)^2 \tag{4}$$

Where MSE is a mean square error, CMI is the cover medical image, and WMI is the watermarked medical image, respectively.

The robustness of the watermarking scheme can be measured by normalized correlation (NC). The normalized correlation can be calculated using eq. 5. NC measures the similarity between the original watermark image and the extracted watermark image. The robustness of any watermarking scheme is high if NC value is close to one.

$$NC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} w(x,y) \times w^*(x,y)}{\sum_{x=1}^{M}\sum_{y=1}^{N} w^2(x,y)} \tag{5}$$

Where, w is original watermark image and w^* is extracted watermark image.

Using the above measures, the imperceptibility test and robustness test of the proposed scheme are performed for various medical images. Further, the strength of Arnold scrambling encryption method is measured by parameters like a number of changing pixel rage (NPCR) [34] and unified average changes intensity (UACI) [34].

5.2 Imperceptibility test

An imperceptibility of the proposed scheme is tested using different cover medical images (shown in Fig. 2). In this test, the performance of the proposed scheme to check how degradation is appearing in the medical image after watermark image inserting into it. For this test, PSNR is calculated between the original cover medical image and watermarked medical image while NC is calculated between the original watermark image and extracted watermark image. Figs. 4 and 5 show resultant images using the proposed scheme for various watermark images such as binary logo and sample patient information using gain factor $\alpha = 0.2$ and $\alpha = 0.5$, respectively.

In the proposed scheme, the performance of the watermark embedding process depends on the gain factor α. The gain factor affects the quality of watermarked medical images and extracted watermark images. Here, the range of gain factor α varies from o.1 to 1, as per the human visual system (HVS) property of watermarking requirements. The performance of the proposed scheme in term of PSNR and NC values are summarized in Table 1. Table 1 presents the values of PSNR, NC, NPCR, and UACI for various watermark images such as binary logo and sample patient information at various gain factor values. Referring to Table 1, it indicates that PSNR value is large for low gain factor value and small for high gain factor value. While NC value is small for low gain factor and high for high gain factor value. These results in Table 1 (a & b) are generated using cover medical images shown in Figs. 4, 5 respectively. The maximum value of PSNR is 58.6703 dB (for gain factor $\alpha = 0.1$) and maximum value of NC is 1 (for gain factor $\alpha = 0.2$ to 1) for this proposed scheme.

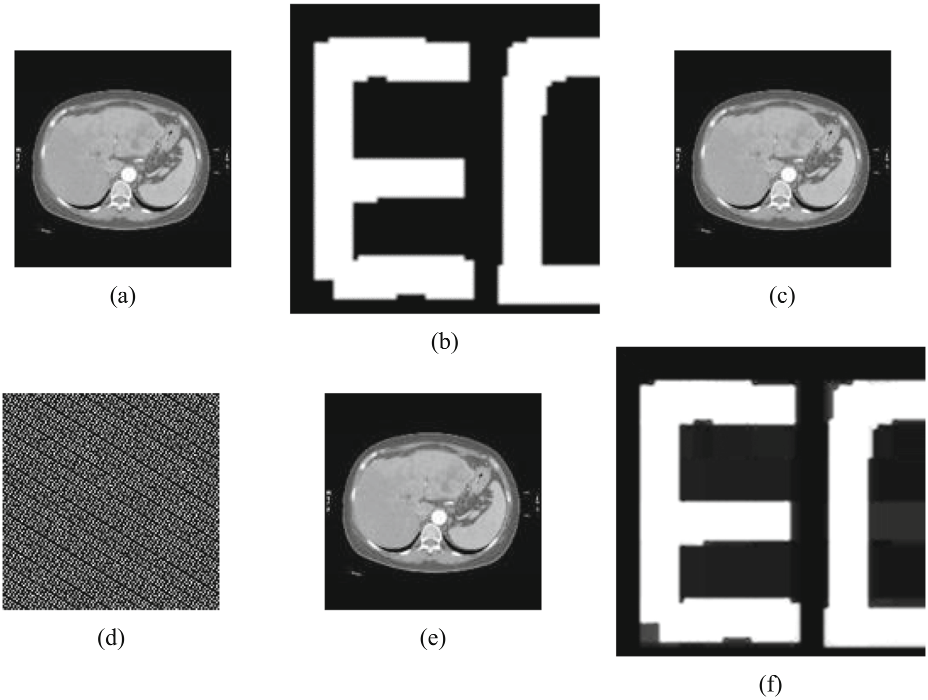


Fig. 4 Resultant Images using Proposed Scheme for Binary Logo using Gain Factor $\alpha = 0.2$ (a) Original Body CT Image (a) Original Watermark Binary Logo (c) Watermarked Body CT Image (d) Encrypted Watermarked Body CT Image (e) Decrypted Watermarked Body CT Image (f) Recovered Watermark Binary Logo

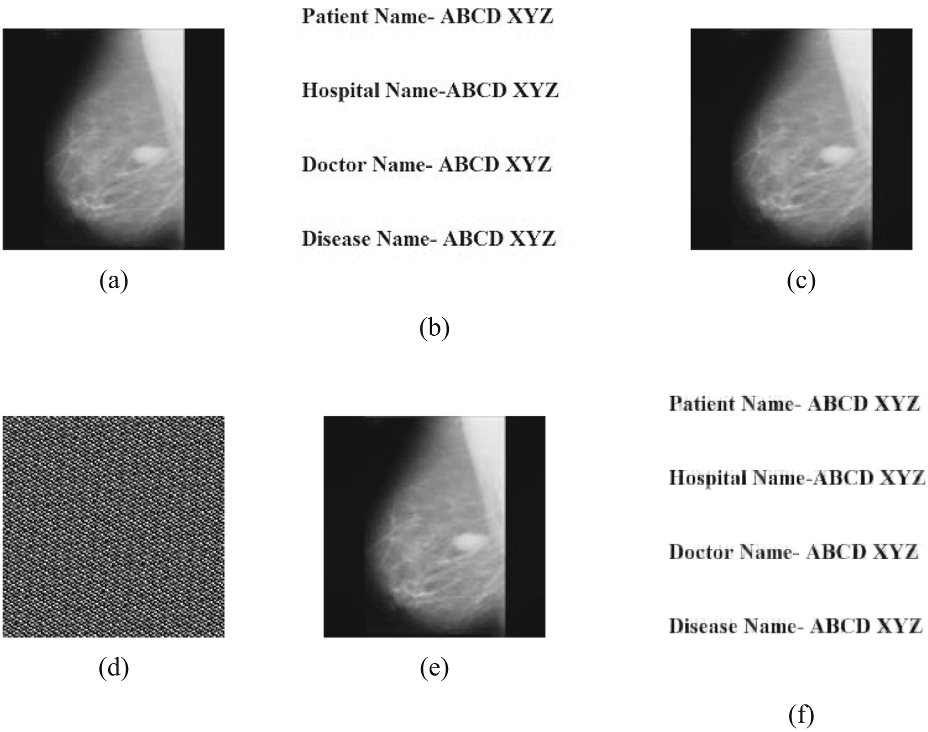


Fig. 5 Resultant Images using Proposed Scheme for Sample Patient Information using Gain Factor $\alpha = 0.5$ (a) Original Breast Mammography Image (a) Original Sample Patient Information (c) Watermarked Breast Mammography Image (d) Encrypted Watermarked Breast Mammography Image (e) Decrypted Watermarked Breast Mammography Image (f) Recovered Sample Patient Information

Also, the Performance of this proposed scheme is tested for various types of cover medical images and tabulated in Table 2. These results in Table 2(a) and 2(b) are generated using a binary logo with gain factor $\alpha = 0.2$ and sample patient information with gain factor $\alpha = 0.5$. Table 2 indicates that the body CT image provides the best PSNR value and NC value such as 52.8761 and 1.000 for the proposed scheme. It is also indicated that the achieved NPCR values and UACI values are better than predefined values [34].

Table 1 Performance of Proposed Scheme at Various Gain Factor Values and Various Watermark Images

Gain Factor	**PSNR (dB)**	**NC**	**NPCR**	**UACI**	**Avg. of NPCR & UACI**
(a) For Binary Logo					
0.1	58.6703	0.5882	0.8566	0.2788	0.5677
0.2	52.8761	1.0000	0.8564	0.2799	0.5682
0.5	45.6115	1.0000	0.8564	0.2821	0.5693
0.8	41.4947	1.0000	0.8552	0.2845	0.5699
1.0	39.5837	1.0000	0.8579	0.2861	0.5720
(b) For Sample Patient Information					
0.1	55.5015	0.5652	0.8387	0.3068	0.5728
0.2	49.0112	0.9973	0.8951	0.3052	0.6002
0.5	41.8189	0.9988	0.9316	0.3024	0.6170
0.8	37.8469	0.9987	0.9498	0.2999	0.6249
1.0	35.9455	0.9988	0.9555	0.2990	0.6273

Table 2 Performance of Proposed Scheme for Various Cover Medical Images

Test Cover Medical Image	PSNR (dB)	NC	NPCR	UACI	Avg. of NPCR & UACI
(a) For Binary Logo					
Body CT	52.8761	1.0000	0.8564	0.2799	0.5682
Neck X-ray	52.7319	0.9705	0.9329	0.3434	0.6382
Brain MRI	52.4147	0.9509	0.8665	0.3463	0.6064
Breast Mammography	51.6473	1.0000	0.8353	0.3079	0.5716
US	51.6567	0.9478	0.8438	0.3214	0.5826
(b) For Sample Patient Information					
Body CT	42.7513	0.9932	0.9094	0.2823	0.5959
Neck X-ray	42.2494	0.9987	0.9595	0.3388	0.6492
Brain MRI	41.8552	0.9923	0.9005	0.1444	0.5225
Breast Mammography	41.8189	0.9988	0.9316	0.3024	0.6170
US	41.2284	0.9893	0.8920	0.2150	0.5535

Also, the PSNR values of the proposed scheme are compared with PSNR values of existing medical image watermarking schemes reported in [26, 27] and tabulated in Table 3. The comparison of the scheme is performed by test images given in paper [26, 27] (shown in Fig. 6). Further, the PSNR values of the proposed scheme are compared with PSNR values of existing image watermarking schemes reported in [9, 10] and tabulated in Table 4. The comparison of these schemes is performed by value standard images which are obtained from public image databases such as the SIPI database [33]. The comparison in Table 3 and 4 shows the proposed scheme provides better imperceptibility to existing medical image watermarking schemes [26, 27] and image watermarking schemes [9, 10].

5.3 Robustness test

For robustness test of the proposed scheme, various watermarking attacks such as JPEG compression, the addition of Gaussian noise, the addition of salt & peppers noise, addition of speckle noise, median filtering, Gaussian low pass filtering, motion blurring, and geometric attacks such as scaling, rotation are applied on watermarked medical image. At the extraction side, if the extraction of the watermark image is possible from a corrupted decrypted watermarked medical image then the scheme is robust and authentic in nature. In this paper, the robustness of the proposed scheme against various watermarking attacks is measured by normalized correlation (NC). The robustness performance of the proposed scheme for various watermark images against various attacks is summarized in Table 4. Table 4 shows that the NC values of the proposed scheme for all types of attacks are greater than 0.7500 which indicates that this scheme provides robustness against various types of attacks.

Figure 7 shows the corrupted watermarked medical images after applying attacks on it and extracted watermark images from the corrupted watermarked medical images. The results

Table 3 Comparison of PSNR (dB) Values of Proposed Scheme with Existing Medical Image Watermarking Schemes [26, 27]

Gain Factor	Existing Scheme [27]	Existing Scheme [26]	Proposed Scheme
0.1	34.6099	39.1402	**57.3996**
0.5	20.6305	39.3049	**43.8387**

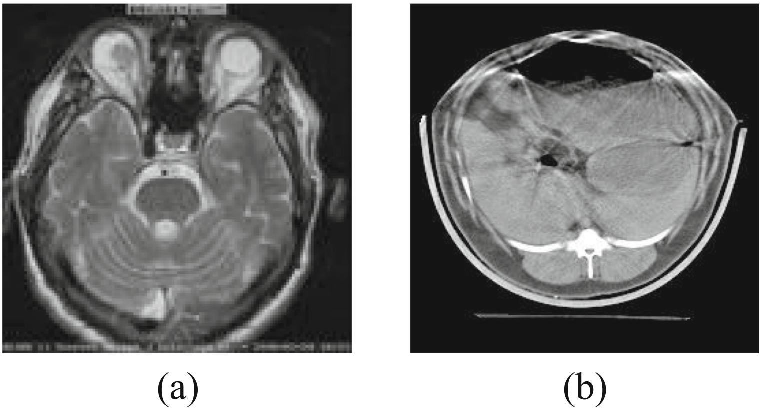


Fig. 6 Test Images of Existing Schemes [26, 27] (a) Cover Medical Image (b) Watermark Medical Image

shown in Fig. 7 are generated using test images reported in [26, 27] for a better comparison of the proposed scheme with these existing schemes.

Also, the NC value of the proposed scheme is compared with NC value of the existing medical image watermarking schemes [26, 27] for the same set of test medical images and summarized in Table 5. The comparison in Table 5 shows that the proposed scheme provides better robustness to existing medical image watermarking schemes [26, 27] against various watermarking attacks.

5.4 Computation time of proposed scheme

The computational time of the encryption method in the watermarking scheme is one of the important parameters because it includes an additional process in conventional watermarking. The speed of the watermarking scheme can't increase due to the encryption method [30]. The time required for encryption and decryption for different cover medical images at gain factor =

Table 4 Robustness Performance of Proposed Scheme against Various Watermarking Attacks

Watermarking Attacks	Quality Parameters	For Binary Logo	For Sample Patient Information
JPEG	Q = 90	0.9859	0.9988
	Q = 70	0.9704	1.0000
	Q = 50	0.9635	0.9898
	Q = 10	0.9375	0.9656
Gaussian Noise	Noise Density = 0.0001	0.9694	1.0000
	Noise Density = 0.0005	0.9663	1.0000
Salt & Pepper Noise	Noise Density = 0.0001	0.9940	0.9480
	Noise Density = 0.0005	0.9592	0.9895
Speckle Noise	Noise Density = 0.0001	0.9933	0.9632
	Noise Density = 0.0005	0.9961	0.9404
Median Filter	Filter Mask = 1 × 1	1.0000	0.9564
	Filter Mask = 2 × 2	0.9618	0.7614
Motion Blurring	–	0.9285	0.8518
Sharping	–	1.0000	0.9516
Scaling	128–256 – 128	0.9452	0.9415
Rotation	1°	0.9974	0.9588
Gaussian Low Pass Filter	Filter Mask = 3 × 3	0.9501	0.8704

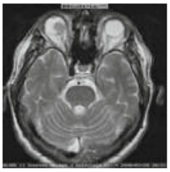
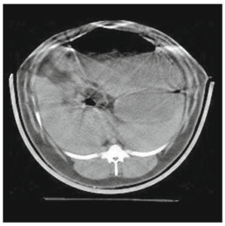
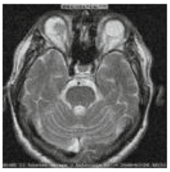
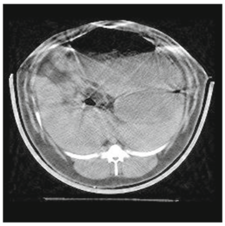
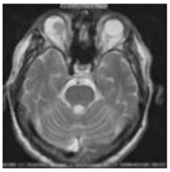
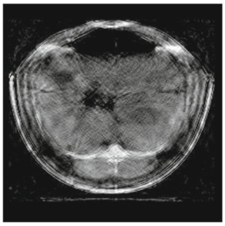
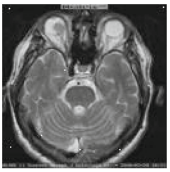
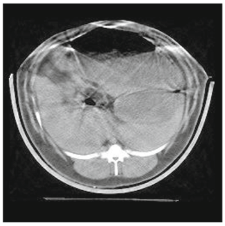
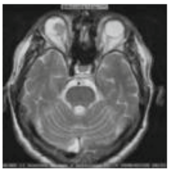
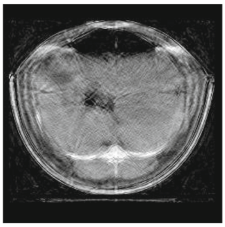
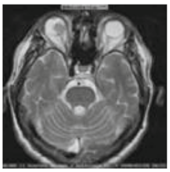
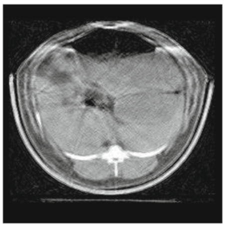
Watermarking Attacks	Corrupted Watermarked Medical Images	Extracted Watermark Images
JPEG Compression (Q = 90)		
Gaussian Noise (Noise Density = 0.0005)		
Median Filtering (2×2)		
Salt & Pepper (Noise Density = 0.0005)		
Gaussian Low Pass Filtering (3×3)		
Scaling		

Fig. 7 Robustness Performance of Proposed Scheme against Various Watermarking Attacks

Table 5 Comparison of NC Values of Proposed Scheme with Existing Medical Image Watermarking Schemes [26, 27]

Attacks	Gain Factor	Noise Density	Existing Scheme [27]	Existing Scheme [26]	Proposed Scheme
Salt & Pepper Noise	0.7	0.04	0.9736	0.9734	**1.0000**
	0.9	0.06	0.9646	0.9641	**1.0000**
Gaussian Noise	0.7	0.04	0.9849	0.9841	**1.0000**
	0.9	0.06	0.9888	0.9872	**1.0000**
Speckle Noise	0.7	0.04	0.9522	0.9496	**1.0000**
	0.9	0.06	0.9285	0.9275	**0.9948**

0.2 is summarized in Table 6 and compared with the time of the existing method [27]. Table 6 indicated that the minimum time and maximum time for encryption are 0.6315 s (for Breast mammography image), 0.7227 s (for Body CT image), respectively while minimum time and maximum time for decryption are 0.3734 s (for Brain MRI Image) and 0.4989 s (for Breast mammography image). Table 6 also indicates that the computational time for the encryption and decryption process of the proposed scheme is less than the computation time of the existing method [27] which is indicated that the proposed scheme performs fast than the existing scheme [27].

5.5 Payload capacity of proposed scheme

The payload capacity (PC) of any watermarking scheme is defined by how much watermark information can embed into a cover medical image. The payload capacity of any watermarking scheme is calculated using the below equation:

$$PC = \frac{W_{Size}}{C_{Size}} bpp \tag{6}$$

where PC is a payload capacity, W_{size} is the size of the watermark image in terms of bits, C_{size} is the size of the cover medical image in terms of pixels, and bpp is bit per pixel.

The payload capacity of the proposed scheme is compared with various existing watermarking schemes [1, 20, 26, 27] and summarized in Table 7. The payload capacity of existing schemes is a half bit per pixel or one bit per pixel while the payload capacity of the

Table 6 Encryption and Decryption Time of Proposed Scheme for Different Medical Images

Test Cover Medical Image	Proposed Scheme		Existing Scheme [27]	
	Encryption Time (seconds)	Decryption Time (seconds)	Encryption Time (seconds)	Decryption Time (seconds)
Body CT	0.7227	0.4180	29.4558	29.21426
Neck X-ray	0.6733	0.4287	29.6230	29.2142
Brain MRI	0.6364	0.3734	30.1990	30.7440
Breast Mammography	0.6315	0.4989	Not reported	Not reported
US	0.6595	0.4887	29.4237	29.1841

Table 7 Comparison of Payload Capacity of Proposed Scheme with Existing Watermarking Schemes [1, 20, 26, 27]

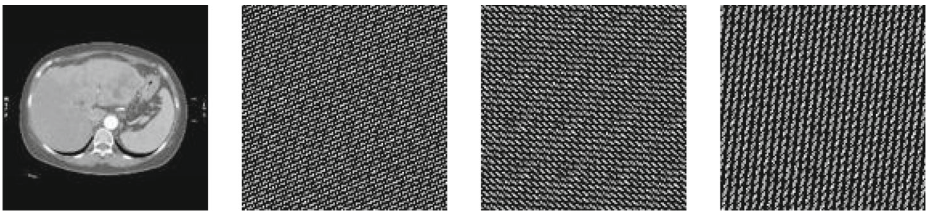
Watermarking Scheme	Size of Watermark Image	Size of Cover Image	Payload Capacity (bpp)
Arunkumar et al. [1]	256 × 256	512 × 512	0.5
Priya et al. [20]	256 × 256	256 × 256	1
Thakur et al. [27]	256 × 256	256 × 256	1
Thakur et al. [26]	256 × 256	256 × 256	1
Proposed	256 × 256	128 × 128	2

proposed scheme is two-bit per pixel. This indicates that the proposed scheme can embed more information compared to existing schemes [1, 20, 26, 27] in the literature.

5.6 Security analysis and false positive test (FPT) of the proposed scheme

In the proposed scheme, the security of the watermarked medical image provided by an encryption algorithm. The Arnold scrambling based encryption and decryption process is used for this purpose. For security analysis of the proposed scheme, Arnold scrambling with secret key $k = 5$ are used for the generation of encrypted watermarked medical images at the transmission side and decrypted watermarked medical images at the receiver side. Fig. 8 (a) shows the decrypted watermarked Body CT image with the correct secret key $k = 5$ while Fig. 8 (b) – (d) shows decrypted watermarked Body CT images using wrong secret keys k^*. The results in Fig. 6 shows that without the correct secret key k, the original watermarked medical image can't be decrypted and obtained at the receiver side. Thus, it indicates that the proposed scheme provides security to the watermarked medical image when it transmits over an open communication channel and used in various telemedicine applications where the security of medical images is required.

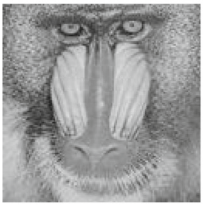
A false positive test (FPT) is a very important test for performance evaluation of SVD based watermarking scheme as per the security requirements of watermarking. Thus, the FPT of the proposed scheme is tested by taking different grayscale images. A false positive (FP) occurs when the watermark is extracted from an unwatermarked grayscale image, which doesn't have actual information of watermark [32]. For analysis of this test, various non-watermarked grayscale image form SIPI database [8] and watermark image, the proposed scheme is applied on each one of test image using same testing parameters such as security keys, gain factor, etc. to try recover watermark image from an unwatermarked grayscale image. The result of this test of the proposed scheme is summarized in Table 8. The result indicates that by assuming that FP occurs if the NC value of recovered watermark image is almost zero; an FP rate for the



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

Fig. 8 Decrypted Watermarked Medical Image using Various Secret Keys (a) $k = 5$ (b) $k = 15$ (c) $k = 30$ (d) $k = 45$

Table 8 Results of False Positive Test (FPT) for Proposed Scheme

Sl. No	Non-watermarked Grayscale Image	Extracted Watermark Image using Proposed Scheme	NC
1			0
2			0
3			0

proposed scheme is zero when it tested on around 30 grayscale images of the SIPI database [33]. According to COX [8], “A false positive rate of 10^{-6} can meet the security requirements” and hence this proposed scheme can meet the security requirements of watermarking.

6 Conclusions

In this paper, a novel non-blind, robust, and high payload capacity based medical image watermarking scheme using FRT and SVD is proposed. In this scheme, the additional security to medical image provides using Arnold scrambling after watermark embedding into it. The obtained evaluation parameters are acceptable as per all requirements of the watermarking and encryption method. The experimental results of the scheme indicated that this scheme is robust against various watermarking attacks. These results are also measuring at different gain factors which are indicated that this scheme equally works for all possible combinations of gain factors. Therefore, the proposed scheme can be used for the security of the medical image in telemedicine applications by exploring the watermarking and encryption method. Further, the comparative analysis of the proposed scheme with existing schemes indicated that the proposed scheme performed better than existing schemes related to the security of medical images.

References

1. Arunkumar S, Subramaniyaswamy V, Vijayakumar V, Chilamkurti N, Logesh R (2019) SVD-based robust image Steganographic scheme using RIWT and DCT for secure transmission of medical images. Measurement. 139:426–437
2. Ashour AS, Dey N (2017) Security of multimedia contents: A brief. In *Intelligent Techniques in Signal Processing for Multimedia Security* (pp. 3–14). Springer, Cham
3. Babu S, Kapinaiah V (2019) Medical image authentication using quartic digital signature algorithm. International Journal of Intelligent Information Systems 7(4):38–41
4. Banerjee S, Chakraborty S, Dey N, Pal AK, Ray R (2015) High payload watermarking using a residue number system. International Journal of Image, Graphics and Signal Processing 3:1–8
5. Borra S, Lakshmi HR (2015) Visual cryptography based lossless watermarking for sensitive images. In *International Conference on Swarm, evolutionary, and memetic computing* (pp. 29-39). Springer, Cham
6. Borra S, Thanki R (2019) Crypto-watermarking scheme for tamper detection of medical images. Computer Methods in Biomechanics and Biomedical Engineering*:* Imaging & Visualization, 1–11
7. Borra S, Thanki R (2019) A FRT-SVD based blind medical watermarking technique for telemedicine applications. Int J Digit Crime Foren (IJDCF) 11(2):13–33
8. Cox IJ, Miller ML, Bloom JA (2000) Watermarking applications and their properties. In *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on* (pp. 6-10). IEEE
9. Kim C, Shin D, Leng L, Yang CN (2018) Separable reversible data hiding in encrypted halftone image. Displays 55:71–79
10. Kim C, Shin D, Leng L, Yang CN (2018) Lossless data hiding for absolute moment block truncation coding using histogram modification. J Real-Time Image Proc 14(1):101–114
11. Kutter M, Petitcolas FA (1999) Fair benchmark for image watermarking systems. In *Security and Watermarking of Multimedia Contents* (Vol. 3657, pp. 226-240). International Society for Optics and Photonics
12. Leng L, Zhang J, Khan MK, Chen X, Alghathbar K (2010) Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain. Int J Phys Sci 5(17):2543–2554
13. Leng L, Zhang J, Chen G, Khan MK, Alghathbar K (2011) Two-directional two-dimensional random projection and its variations for face and palmprint recognition. In *International conference on computational science and its applications* (pp. 458-470). Springer, Berlin, Heidelberg
14. Leng L, Zhang S, Bi X, Khan MK (2012) Two-dimensional cancelable biometric scheme. In *2012 International Conference on Wavelet Analysis and Pattern Recognition* (pp. 164-169). IEEE
15. Leng L, Li M, Kim C, Bi X (2017) Dual-source discrimination power analysis for multi-instance contactless palmprint recognition. Multimed Tools Appl 76(1):333–354
16. Li M, Liang T, He YJ (2013) Arnold transform based image scrambling method. In: 3rd International Conference on Multimedia Technology. Atlantis Press, China, pp 1302–1309
17. Medical Image Database. Available: https://medpix.nlm.nih.gov/. Last Access Year: 2017
18. Menon V, Du Q, Fowler JE (2016) Fast SVD with random Hadamard projection for hyperspectral dimensionality reduction. IEEE Geosci Remote Sens Lett 13(9):1275–1279
19. Pirbhulal S, Samuel OW, Wu W, Sangaiah AK, Li G (2019) A joint resource-aware and medical data security framework for wearable healthcare systems. Futur Gener Comput Syst 95:382–391
20. Priya S, Santhi B (2019) A novel visual medical image encryption for secure transmission of authenticated watermarked medical images. *Mobile Networks and Applications*, 1–8
21. Roy S, Pal AK (2017) A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling. Multimed Tools Appl 76(3):3577–3616
22. Singh, A. K., Kumar, B., Singh, G., & Mohan, A. (Eds.). (2017). Medical image watermarking: techniques and applications. Springer
23. Singh S, Singh R, Singh AK, Siddiqui TJ (2018) SVD-DCT based medical image watermarking in NSCT domain. In *Quantum Computing: An Environment for Intelligent Large-Scale Real Application* (pp. 467–488). Springer, Cham
24. Suckling J (1994) The mammographic image analysis society digital mammogram database. *Exerpta Medica*. Int Congr Ser 24(1069):375–378
25. Surekha B, Swamy GN (2011) A spatial domain public image watermarking. International Journal of Security and Its Applications 5(1):1–12
26. Thakur S, Singh AK, Ghrera SP, Mohan A (2018) Chaotic based secure watermarking approach for medical images. *Multimedia Tools and Applications*, 1–14
27. Thakur S, Singh AK, Ghrera SP, Elhoseny M (2019) Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimed Tools Appl 78(3):3457–3470

28. Thanki R, Borra S (2018) A color image steganography in hybrid FRT–DWT domain. J inform secur appl 40:92–102
29. Thanki R, Borra S (2018) Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing. *Multimedia Tools and Applications*, 1–20
30. Thanki, R., & Borra, S. (2019). Medical imaging and its security in telemedicine applications. Springer International Publishing
31. Thanki RM, Kothari AM (2017) Digital watermarking: technical art of hiding a message. *Intelligent analysis of multimedia information* (pp. 431–466). IGI global
32. Thanki R, Borra S, Dwivedi V, Borisagar K (2017) An efficient medical image watermarking scheme based on FDCuT–DCT. Eng Sci Technol Int J 20(4):1366–1379
33. University of South Carolina SIPI Image Database: http://sipi.usc.edu/database/database.php, Last Access Year: 2017
34. Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) 1(2):31–38

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Dr. Rohit Thanki is a computer vision expert and AI researcher with more than 5 years of work experience in areas of computer vision, medical image analysis & security, artificial intelligence and biometrics including 2 years of academic experience in various engineering institutions in India. Presently, he is working as a research & development director, Prognica Labs Tech FZCO, Dubai Silicon Oasis, Dubai, UAE. He earned his bachelors in electronics & communication, masters in communication engineering and a doctorate degree in electronics & communication with a specialization in digital image processing and biometric security. His areas of research interest are medical image analysis, artificial intelligence, machine learning, deep learning, digital watermarking, biometric security, and compressive sensing. He has more than 40 publication in his create and has published in reputed journals with high impact factor and international conferences which indexing in Scopus / SCIE / WOS. Also, He has authored and contribute in more than 20 books with reputed publishers, i.e., Springer, CRC press, Elsevier, De Gruyter, and IGL Global. He has been invited as reviewer in various reputed journals such as ACM Transactions on Multimedia Computing, Communications and Applications, IEEE Consumer Electronics Magazine, IEEE Access, IEEE Journal of Biomedical and Health Informatics, International Journal of Network Management, Pattern Recognition, Computers and Electrical Engineering, Informatics in Medicine, Journal of Ambient Intelligence and Humanized Computing, IET Biometrics, and IET Image Processing.

Dr. Ashish Kothari is a currently a deputy registrar in Atmiya University, Rajkot, India. He is also a HOD of Department of Electronics and Communication Engineering of Atmiya Institute of Technology and Science, Rajkot. He received Doctorate in "Digital Video Watermarking" from JJTU, Rajasthan, India. His current research interests are Image Processing, Computer Vision, Machine Learning, Robotics and Internet of things. He has filed more than 5 India patents, published 4 books, and several several research papers to her credit in refereed & indexed journals, and conferences at international level.His international recognition includes his professional memberships & services in refereed organizations, program committees and reviewer for journals.