

A Triple-Channel Encrypted Hybrid Fusion Technique to Improve Security of Medical Images

Ahmed S. Salama^{1,2,3}, Mohamed Amr Mokhtar³, Mazhar B. Tayel³,
Esraa Eldesouky^{4,6} and Ahmed Ali^{5,6,*}

¹Future University in Egypt, Cairo, Egypt

²Cairo Higher Institute for Engineering, Computer Science and Management, Cairo, Egypt

³Department of Electrical Engineering, Faculty of Engineering, Alexandria University, Alexandria, 21544, Egypt

⁴Department of Computer Science, Faculty of Computers and Informatics, Suez Canal University, Ismailia City, Egypt

⁵Higher Future Institute for Specialized Technological Studies, Cairo, Egypt

⁶Department of Computer Science, College of Computer Engineering and Sciences,
Prince Sattam Bin Abdulaziz University, Al-Kharj, 11942, Saudi Arabia

*Corresponding Author: Ahmed Ali. Email: a.abdallah@psau.edu.sa

Received: 25 December 2020; Accepted: 26 January 2021

Abstract: Assuring medical images protection and robustness is a compulsory necessity nowadays. In this paper, a novel technique is proposed that fuses the wavelet-induced multi-resolution decomposition of the Discrete Wavelet Transform (DWT) with the energy compaction of the Discrete Wavelet Transform (DCT). The multi-level Encryption-based Hybrid Fusion Technique (EbHFT) aims to achieve great advances in terms of imperceptibility and security of medical images. A DWT disintegrated sub-band of a cover image is reformed simultaneously using the DCT transform. Afterwards, a 64-bit hex key is employed to encrypt the host image as well as participate in the second key creation process to encode the watermark. Lastly, a PN-sequence key is formed along with a supplementary key in the third layer of the EbHFT. Thus, the watermarked image is generated by enclosing both keys into DWT and DCT coefficients. The fusions ability of the proposed EbHFT technique makes the best use of the distinct privileges of using both DWT and DCT methods. In order to validate the proposed technique, a standard dataset of medical images is used. Simulation results show higher performance of the visual quality (i.e., 57.65) for the watermarked forms of all types of medical images. In addition, EbHFT robustness outperforms an existing scheme tested for the same dataset in terms of Normalized Correlation (NC). Finally, extra protection for digital images from against illegal replicating and unapproved tampering using the proposed technique.

Keywords: Medical image processing; digital image watermarking; discrete wavelet transforms; discrete cosine transform; encryption image fusion; hybrid fusion technique



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

Digital image watermarking is a primary way to discriminate multi-media contents (i.e., images, video clips, texts, or audio), by concealing critical information [1–3]. Frequency-domain watermarking is a type of watermarking techniques in which the transform coefficients rely directly on changing pixel values [4]. Thus, inverse transform aims to restore the identity of the encrypted watermark. Popular transforms used in the frequency-domain includes Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Fast Fourier Transform (FFT), and Discrete Fourier Transform (DFT) [5–8]. The least significant bits (LSB) is a recent technique that adjusts the least significant bits of the image's pixel [9]. The high rendering capability of DWT in spatial localization allows it to be widely employed in image watermarking [5]. Besides, the pixel values of the image are changed directly on the watermark prior to embedding in spatial domain techniques.

The proposed technique points to enhance image robustness as well as imperceptibility against some sort of attacks which are the main advantages of DWT technique. The fusion of DWT and DCT can fulfil extra performance enhancements in image watermarking calculations. The blocking artifact relies on a parallel coalition of cosine and wavelet transforms which results when boundaries between sub-images become visible [5]. In the proposed technique, the host image is subdivided into DWT sub-bands simultaneously another transform is taking place using DCT method. Moreover, image protection and robustness are ensured by embedding the secret data in the decomposed region with keys [10]. Such taming conceivably replenishes the drawbacks of utilizing each method individually drawing out an effective watermarking technique [11].

A significant number of studies uses the correlation of PN sequences for blind extraction of the watermark. Similarly, other studies evaluate the robustness tests evaluate capacity to withstand various attacks for existing watermarking techniques. However, the proposed technique aims to design a new powerful watermarking technique that conquers the mentioned problems regarding watermarking.

The remainder of this paper is organized as follows: next section summarizes the literature work. The preliminaries are presented in Section 3 whereas detailing the procedures required for embedding and extracting watermarks in the EbHFT technique is exhibited in Section 4. Afterwards, experimental results and performance measures are analyzed in Section 5. Finally, the paper is concluded in Section 6.

2 Literature Review

Recent pertinent research work is presented along with putting an eye on their shortcomings. RSA-Discrete Wavelet Transform (DWT), DWT-Artificial Neural Network (ANN) and DWT-SVD are popular medical images watermarking techniques which were compared in [12]. This precious comparison demonstrated that the DWT-SVD technique performed other two techniques. A robust watermarking technique for medical images security is proposed in [13] that huddles wavelet change, neural system and Rivest–Shamir–Adleman (RSA) encryption-based. This technique aims to recoup an outface watermark and progressively secure by hiding it into the host image's wavelet sub-bands using the neural networks. In [14], a block SVD and wavelet transform-based blind a watermarking scheme is introduced, which also targets the security of medical images. Consequently, a watermarked image as well as Electronic Patient Record (EPR) are jointly inset into the singular values in the host image of its wavelet sub-bands. Although, this scheme

verifies robustness against all possible watermarking attacks, it is only applicable for Region of Interest (ROI) of therapeutic images.

A second combined mechanism that emphasizes sturdy watermarking in medical images is proposed by fusing SVD, DWT and cryptographic methods [15]. An encoded watermarking data (i.e., using Reed-Solomon, Bose–Chaudhuri–Hocquenghem and Hamming code) is embedded into the wavelet-coefficients and in the singular value of the targeted medical image. However, the Reed–Solomon-based coding for watermarked data much better than other tested codes. Fuzzy logic and Harris corner detection are also utilized as a hidden watermarking technique for medical images [16]. Alternatively, a medical hidden medical information scheme is presented which is based on particle swarm optimization [17]. This study is an enhancement for the use of the three PN sequences which depends on watermark bits to improve imperceptibility [18].

A robust watermark protection scheme that utilizes Fast Discrete Curvelet Transform (FDCuT) is proposed whereas binary watermark data is embedded into low frequency curvelet coefficients [19]. Another watermarking method that preserves copyright protection during image hash is figured using curvelet transform [20,21]. The presented hash esteems are maintained into different level of curvelet transform for the host image. A blended watermarking technique is proposed which combines blind FDCuT, DCT, and White Gaussian Noise sequences for medical images [22]. The mid-band frequency DCT coefficients of a medical image curvelet sub-band is modified according to two WGN sequences whereas watermark blind extraction can be obtained at detector side.

Discovering the ROI of a host image and changing it to non-overlapping blocks is proposed for achieving carefully watermark medical images [23]. A study introduced medical image hybrid protection watermarking schemes, which are based on DWT, SVD and spread spectrum approach [18,24]. This research study depicted two techniques using the correlation property of PN sequences to obtain blind extraction. In the first one, the sub-bands of host medical image (i.e., horizontal and vertical) are changed by two PN sequence according to its watermark bits. The other one concern a singular value of wavelet sub-bands of host medical image which is changed by two PN sequences based on the watermark bits. Later, Bose–Chaudhuri–Hocquenghem (BCH) encryption is utilized for security of watermark data.

A multi-level encryption-based technique (EbDT) is introduced to integrate the wavelet-induced multiresolution decomposition power of DWT with the energy compaction capability of DCT. This study strives to enhance both medical image robustness and security [25]. The proposed technique is decomposed of three layers in which a DWT decomposed sub-band of an image is adjusted using DCT transform. Afterwards, a 64-bit key is employed to create secure force (SF) key (i.e., K1–K5). The generated keys encrypt the host image and produce a second key for watermark encryption. Finally, a PN-sequence is generated along with an extra key and embedded into the DCT coefficients to deliver the watermarked image.

The techniques presented in the previous literature are majorly based on DWT, SVD, and DCT in order to improve the imperceptibility of watermarked images. However, in this study, a hybrid DCT-DWT technique is presented to defeat the inadequacies of the mentioned literature mainly in [13,18,19,22,25]. Although the two WGN sequence is used in [21], it fails to achieve higher imperceptibility for medical images even for a standard database. As aforementioned, studies proposed in [18,19] used two PN sequences to separate a blind watermark just as correlation. Both methods resulted in poor visual fidelity for the watermarked images. Additionally, in [13] authors succeeded to define predetermined ROI in the host or cattier images. Yet, this

study aims to design a novel robust technique that conquers the above-referred problems in watermarking research.

3 Basic Background

3.1 DCT and DWT

The DCT is considered one of the powerful frequency-domain transform technique in watermarking process. It is primarily utilized in signal and video processing as well as it is also great for audio and images where small high-frequency elements can be dismissed. Knowingly, a finite sequence of data points is expressed as a sum of cosine functions balanced at distinct frequencies. Regarding digital images, the DCT is calculated along with the inverse DCT (i.e., IDCT) [26].

Block-wise and non-block wise partitioning are two common DCT ways, which are employed to images. Keeping-up the image quality can be guaranteed using the mid-band DCT coefficients due to their resilience to watermarking attacks [3,27]. In the proposed EbHFT technique, watermark process depends on applying block-wise DCT technique on high, mid, and low frequency sub-bands of the carrier image.

A complementary technique is the Discrete Wavelet Transform (DWT). In watermarking process, wavelet transforms are mainstream in a large scope of applications since it accomplishes an out-standing multi-resolutions modelling [28–30]. The DWT parcels an original image into vertical, horizontal, diagonal and lower resolution image sub-bands (i.e., LH, HL, HH, and LL, respectively). To understand the multiple scale wavelet decomposition, the image partitioning process is iterated [31]. Later, digital watermarks are embedded in the sub-bands along with the decomposed levels. This process is controlled by a random key that is inserted and recovered autonomously.

The intensity of an image energy is located at high band decomposition levels. This is identical to significantly identify low frequency coefficients while aggregating minor energy portion in the low decomposition levels [32]. Susceptible information in medical images (i.e., patient ID or doctor's signature) should be exposed to high robustness. Thus, inserting the watermark in LH and HL sub-bands guarantees robustness.

At end, DCT and DWT are widespread transforms that mainly constitutes the proposed EbHFT technique.

3.2 SF Encryption Algorithm

The architecture of Secure Force (SF) algorithm allows low-complexity encryption, which is applicable in many fields such as wireless sensor networks and information security. It has been developed from the Feistel algorithm and was firstly proposed by Shamir [33,34]. The encryption process consists of basic operations (i.e., AND, OR, XOR, XNOR, shifting, and swapping) which lessen a burden on the encoder. Consequently, complex key expansion process only takes place at the decoder side. Only five rounds of encryption keys are required for the encryption process whereas less power consumption is gained. Security issues can be ensured through each operation operating on 4-bit data.

Furthermore, the expansion process is implemented at the decoder by creating confusion and diffusion of data to withstand against various attacks. Complex mathematical operations are utilized to obtain keys needed for the encryption process. Nevertheless, generated keys must be passed to the encoder through secure channels.

4 The EbHFT Technique

The proposed EbHFT technique suggests integrating the privileges of both DCT (i.e., energy compaction capacity) along with DWT (i.e., multi-resolution decomposition capacity). Imperceptibility, security, and robustness of medical images are the primary objectives for enhancement using EbHFT. In addition, secure force (SF) keys are employed to encrypt the host image and create a second key that encodes the watermark. The process of inserting and extracting a digital watermark is presented in this section. Initially, the DWT scheme is applied on Harr filter-decomposed coefficients of the host image. Subsequently, the watermark is embedded into the second-layer sub-band of the host image to improve the robustness of the resulting image (i.e., sturdy enough against illegal tampering).

4.1 Watermark Embedding Algorithm

The three-channels watermark embedding procedure of EbHFT performs DWT on the cover and decomposes the host image into two levels [11]. First, LL1, HL1, LH1, and HH1 then smaller sub-bands are decomposed into then LL2 is chosen along with HH1. Afterwards, it selects the LL2 and HH1 sub-bands to apply the DCT on it [32]. As discussed in Fig. 1, using the 64-bit hex key (i.e., Key 1 = '133457799bbcdff1') allows the generation of SF keys (K1–K5) which generate the encrypted host image.

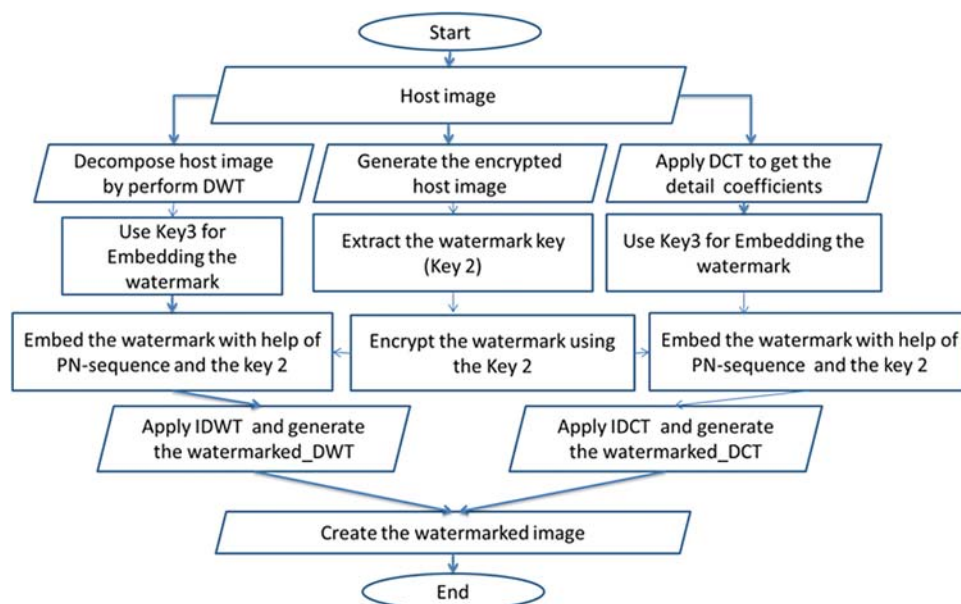


Figure 1: Three-channel watermark embedding flowchart

On one side, the encrypted image is maintained to retrieve the watermark key (i.e., Key2). A PN-sequence is formed from the ciphered watermark and is distributed, then distributing the PN-sequence along with Key 3 on the detailed DWT coefficients. On the other side, performing the Inverse DWT (IDWT) on the transformed image is mandatory to rebuild the watermarked image. This process involves the modified sub-band (i.e., producing the image_DWT) in parallel with spreading the PN-sequence with Key 3 onto the DCT coefficients. After the modification of the mid-band coefficients, IDCT is applied to embed the watermark bits to produce the watermarked

image_DCT. Lastly, the resulting watermarked image_DWT and image_DCT are integrated to generate the final watermarked image.

4.2 Watermark Reconstruction Algorithm

After applying the embedding algorithm for the digital watermark, the extraction algorithm is explained, which is also a three-layers procedure. In the EbHFT technique, the watermark reconstruction algorithm defuses the watermarked image into two images which are watermarked_DWT and watermarked_DCT. As illustrated in Fig. 2, two processes are proceeding in parallel during this stage.

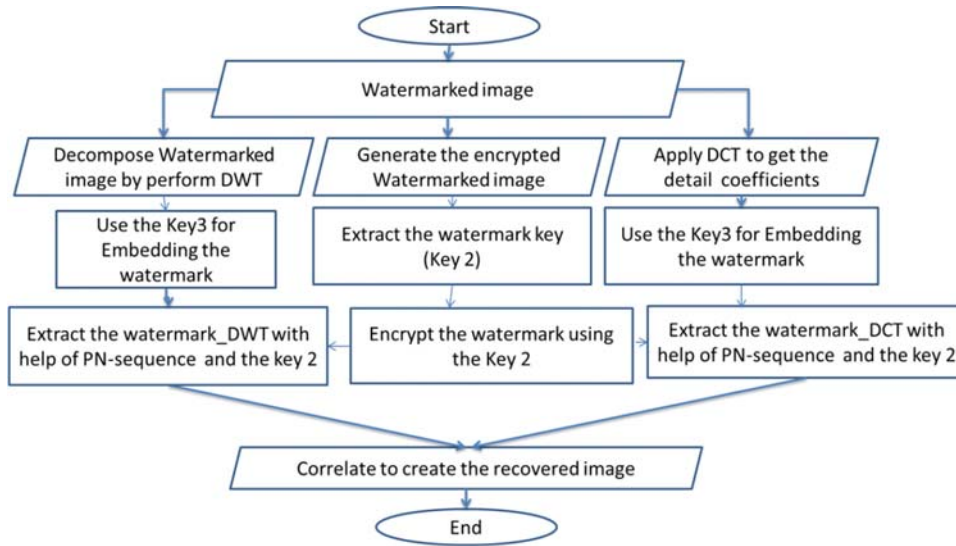


Figure 2: The flowchart of the proposed reconstruction algorithm

The watermarked_DWT image is decomposed using DWT scheme into four multi-resolution sub-bands (i.e., LL1, HL1, LH1, and HH1). Thereafter, DWT is re-applied on the HH1 sub-band to re-split it into smaller four sub-bands. At this instance, the LL2 sub-band is selected in order to achieve superior robustness [32]. Finally, Key 3 is utilized in the detail coefficients of LL2 sub-band using DWT transform to generate the encrypted watermark_DWT. (Finally, Key 3 is utilized under DWT transform to extract the encrypted watermark_DWT by implanting it in the detail coefficient of LL2 sub-band). In parallel with the first process, the DCT is implemented on the watermarked_DCT as described in [32]. Similarly, a certain key (i.e., Key 3) is used in the detail coefficients of DCT scheme to reproduce the encrypted watermark_DCT.

In the third channel, the 64-bit hex key (i.e., Key1 = '133457799bbcdf1') is employed to produce the SF keys (K1–K5) and consequently generate the watermarked image [10]. Later, Key 2 (i.e., watermark key) is taken out from the encrypted watermarked image. Thus, the encrypted watermarks from the DWT and DCT schemes are decrypted using Key 2. The pixel-wise is correlated between the recovered watermark from both DWT and DCT. Accordingly, the recovered watermark image is generated.

5 Results and Analysis

The proficiency of the proposed EbHFT technique is examined on medical images dataset which involves Magnetic Resonant Imaging (MRI), Computerized Tomography (CT), X-ray, and Ultrasound (US) collected from the MedPix™ Medical Image Database [35]. Images included in the experiment are all of resolution 1024×1024 pixels. EbHFT technique is implemented using MATLAB 2016a with a machine of 2.7 GHz i5 CPU with 4 GB-RAM. In Fig. 3, sample images are selected from the dataset (i.e., Figs. 3a–3d) along with the watermark logo and key which are represented in Figs. 3e and 3f, respectively. The used watermark is a simple 20×50 binary image.

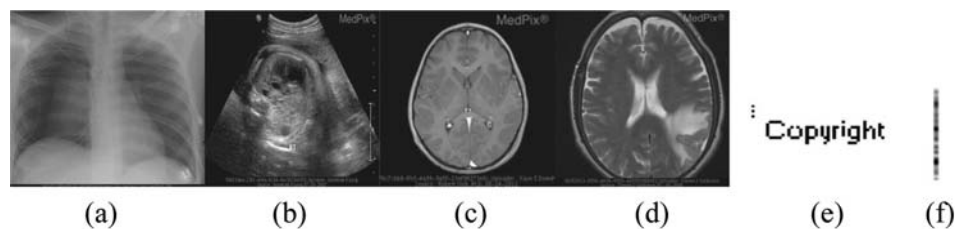


Figure 3: Host medical images: (a) X-ray (b) Ultrasound (US) (c) Magnetic Resonant Imaging (MRI) (d) Computerized Tomography (CT), (e) The ‘Copyright’ watermark image and (f) The embedding key

As mentioned earlier, the watermark is embedded in the detailed DWT wavelet coefficients of the host image using a certain key [11]. Thus, a 64-bit key is maintained to generate the SF keys K1–K5 which are mandatory to construct the encrypted host image [10]. The watermark key (i.e., Key 2) is quarried from the encrypted image and used to cipher the watermark. A PN-sequence is prepared from the encrypted watermark and spread together with Key 3 onto the detailed coefficients of both DCT and DWT. This step is essential for enhancing the image robustness against various attacks.



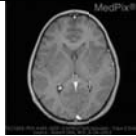
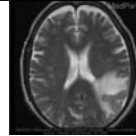



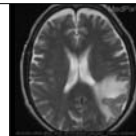



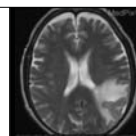


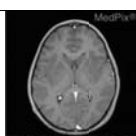
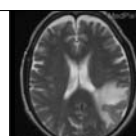



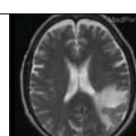


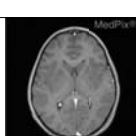

5.1 Performance Metrics

The performance of image-hiding techniques is analyzed based on several metrics including imperceptibility, robustness, noise-addition, filtering attacks as well as JPEG Compression. Tab. 1 illustrates the effect of the proposed technique on the generated watermarked image samples and their recovered watermark. These medical images are tested with our watermark logo under different gain factor G .

5.2 Result Analysis



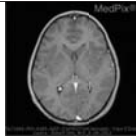
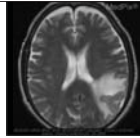






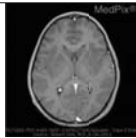
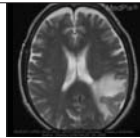




One of the important metrics to measure is the perceptual quality (i.e., imperceptibility) which is estimated by the peak signal to noise ratio (PSNR) between the original host image and the watermarked image. The PSNR mainly relies on the Mean Square Error (MSE) which is measured in dB value. Thus, the error between the original and processed images are calculated in Eqs. (1) and (2), respectively.

Table 1: The output of the watermarked medical images and the corresponding recovered watermark for distinct gain factor G .

Gain Factor	Test Image	X-Ray	US	MRI	CT
G = 2	Watermarked Image				
	Extracted Watermark	: Copyright	: Copyright	: Copyright	: Copyright
G = 4	Watermarked Image				
	Extracted Watermark	: Copyright	: Copyright	: Copyright	: Copyright
G = 6	Watermarked Image				
	Extracted Watermark	: Copyright	: Copyright	: Copyright	: Copyright
G = 8	Watermarked Image				
	Extracted Watermark	: Copyright	: Copyright	: Copyright	: Copyright
G = 10	Watermarked Image				
	Extracted Watermark	: Copyright	: Copyright	: Copyright	: Copyright
G = 15	Watermarked Image				
	Extracted Watermark	: Copyright	: Copyright	: Copyright	: Copyright

(Continued.)

Table 1 (continued).

G = 20	Watermarked Image				
	Extracted Watermark	 Copyright	 Copyright	 Copyright	 Copyright
G = 25	Watermarked Image				
	Extracted Watermark	 Copyright	 Copyright	 Copyright	 Copyright

$$PSNR(I_{org}, I_w) = 10 \times \log \left(\frac{255^2}{MSE(I_{org}, I_w)} \right) \tag{1}$$

$$MSE = \frac{1}{MN} \sum_{j=1}^M \sum_{k=1}^N (X_{j,k} - X'_{j,k})^2 \tag{2}$$

In [Tab. 2](#), a quantitative comparison between the watermarked and host images is introduced which points to the direct relation between the gain factor and the extracted watermark images' quality. Compared to the techniques presented in [\[22,25\]](#) and, the PSNR and NC values studied for the proposed EbHFT technique as in [Figs. 4](#) and [5](#). These comparisons are applied using the factor $k = 2$ without the presence of any attacks.

In [Fig. 4](#), the average of PSNR of the watermarked images of the EbHFT technique is around 57.5 dB. This means that this watermarked image is not affected by the embedded bits of the watermark. Accordingly, the proposed technique achieved compromised imperceptibility in comparable with the other techniques in [\[22,25\]](#). Correspondingly, the NC value of the extracted watermark exhibited in [Fig. 5](#) for the proposed technique is 1 compared to 0.97 for the existing techniques which allow the full recovery for the watermark. This watermark image extraction using the EbHFT outperforms the techniques presented in [\[22,25\]](#).

An essential target is to improve the perceptual quality of the proposed algorithm which indicates higher values of PSNR. The Normalized Cross-Correlation (NCC) is another performance metric measured in [Eq. \(3\)](#) that estimates the distinction between the host and watermarked images.

$$NCC = \frac{\sum_{j=1}^M \sum_{K=1}^N (X_{j,k})(X'_{j,k})}{\sum_{j=1}^M \sum_{K=1}^N X_{j,k}^2} \tag{3}$$

Table 2: Evaluating the proposed EbHFT technique for different values of gain factor (k)

G	Image	MSE	NCC	WDR	PSNR	NAE	NCC for watermark
2	X-ray	0.1315	1	-116.2886	56.9416	0.0011	1
	US	0.1116	1	-107.0583	57.6538	0.0023	0.9893
	MRI	0.1299	1	-109.0987	56.9953	0.0023	1
	CT	0.1309	1	-108.2062	56.9613	0.002	1
4	X-ray	0.5613	1	-101.7768	50.6392	0.0044	1
	US	0.4801	1	-92.4692	51.3178	0.009	0.984
	MRI	0.5416	1	-94.8204	50.7943	0.0086	1
	CT	0.5587	1	-93.6951	50.6593	0.0079	1
6	X-ray	1.0099	1	-95.9021	48.0878	0.0064	1
	US	0.8628	1	-86.6064	48.7716	0.013	0.984
	MRI	0.9316	1	-89.3966	48.4387	0.0122	1
	CT	1.0044	1	-87.8292	48.1117	0.0114	1
8	X-ray	1.828	1	-89.9686	45.511	0.009	1
	US	1.5368	1	-80.834	46.2647	0.018	0.984
	MRI	1.5866	1	-84.0718	46.1262	0.0165	1
	CT	1.8152	1	-81.9113	45.5416	0.0159	1
10	X-ray	2.9157	1	-85.3	43.4834	0.0116	1
	US	2.4311	1	-76.2473	44.2727	0.0233	0.984
	MRI	2.4424	1	-79.7576	44.2526	0.0209	1
	CT	2.8929	1	-77.2506	43.5175	0.0207	1
15	X-ray	6.2974	1	-77.5996	40.1392	0.0174	1
	US	5.2847	1	-68.4827	40.9006	0.0349	0.984
	MRI	5.1591	1	-72.2799	41.0051	0.0303	1
	CT	6.2446	1	-69.556	40.1757	0.0309	1
20	X-ray	11.0743	1	-71.9548	37.6876	0.0232	1
	US	9.2332	1	-62.9028	38.4773	0.0462	0.984
	MRI	8.8666	1	-66.8647	38.6532	0.0393	1
	CT	10.955	1	-63.9352	37.7347	0.0411	1
25	X-ray	17.2455	1	-67.5255	35.764	0.029	1
	US	14.3405	1	-58.5	36.5651	0.0577	0.984
	MRI	13.6524	1	-62.5484	36.7787	0.0483	1
	CT	16.9434	1	-59.5743	35.8408	0.0513	1

Furthermore, Watermark to Document Ratio (WDR) see Eq. (4) and other metrics are used in our experimental study. The first scales the ratio between the watermarked and host images and the second determines the difference between a certain pixel in the original and watermarked images. Finally, the Normalized Absolute Error (NAE) defines the error prediction accuracy of the image as computed in Eq. (5):

$$WDR = 10 \log \frac{\sum_{i=1}^N \sum_{j=1}^N [X(i,j) - X_w(i,j)]^2}{\sum_{i=1}^N \sum_{j=1}^N X(i,j)^2} \quad (4)$$

where $X(i, j)$ is the host image and $XW(i, j)$ is the watermarked image.

$$NAE = \frac{\sum_{j=1}^M \sum_{K=1}^N |X_{j,k} - X'_{j,k}|}{\sum_{j=1}^M \sum_{K=1}^N X_{j,k}} \quad (5)$$

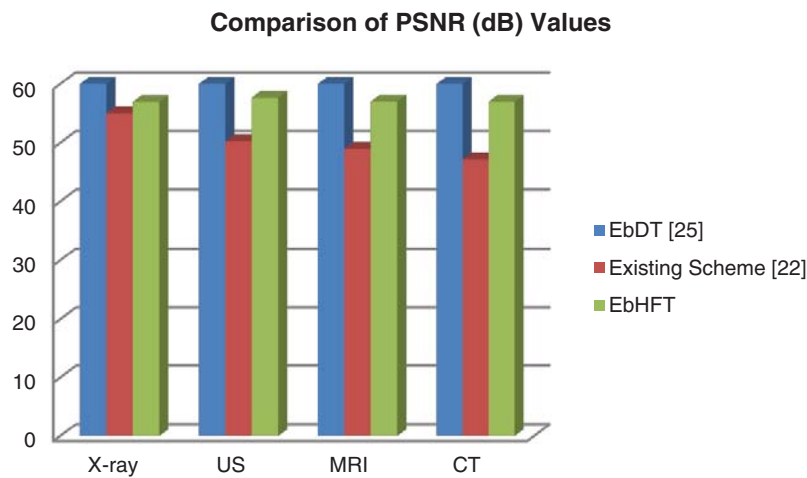


Figure 4: Comparison of PSNR (dB) value of proposed technique with existing technique [22,25] without application of watermarking attacks

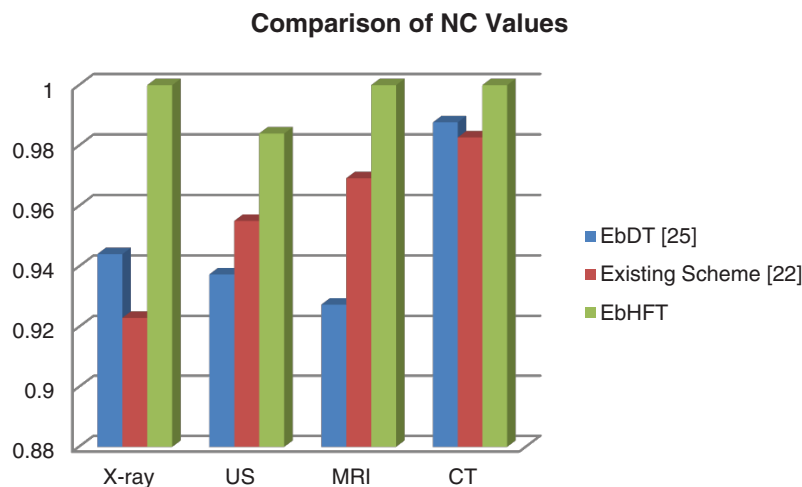


Figure 5: Comparison of NC value of proposed technique with existing technique [22,25] without application of watermarking attacks

In this study, the robustness test is considered an efficient way to assess attacks against the watermarked images such as JPEG compression, filtering, Gaussian low pass filtering. Generally, other attacks can be counted including sharpening, Gaussian noise, speckle noise, and

salt-and-pepper noise. As a result, the applied technique is robust if the generated watermark is visually perceptual. Subsequently, NC values are deemed as a primary measurement for the robustness against attacks in the proposed technique. These values are acquired and compared with the existing techniques [22,25] for the same set of medical images.

The JPEG compression is implemented on the watermarked images along with several quality criteria. At End, the watermark is extracted using the proposed technique. In Tab. 3, the results of compression attacks are presented for distinct medical images (i.e., displayed in Figs. 3a–3d) involving X-rays, Ultrasound, MRI and CT images. These images are accompanied with a watermark logo (i.e., Fig. 3e) and NC to appraise the compression attacks against these images. The conducted results evidence the outperforming of the EbHFT technique. Same selected watermarked images are exposed to diverse sorts of noise attacks such as speckle, salt-and-pepper noise, and Gaussian noise. NC for these attacks and the outcomes are exhibited in Fig. 6. Fig. 7 shows the results of applying filtering attacks (i.e., such as median mean and Gaussian low pass filtering).

Table 3: Comparison of EbHFT technique with existing techniques for various features.

Method features	[13]	[18]	[19]	[22]	[25]	EbHFT
Type of scheme	Robust	Robust	Robust	Robust	Robust	Robust
Number of processing transforms	2	1	1	2	2	2
Transform used to embed watermark	DWT and SVD	DWT	DWT	FDCuT and DCT	DWT and DCT	DWT and DCT
Number of noise sequences	Not used	Three PN sequences	Two PN sequences	Two WGN sequences	Three PN sequences	Three PN sequences
Maximum PSNR (in dB)	31.17	39.03	37.75	55.06	60.84	57.65
Maximum NC	0.6676	0.7409	0.7544	0.9998	1	1
Execution time (in seconds)	Not mentioned	108.92	Not mentioned	29.95	7.88	4.96

The performance assessments are concluded in Fig. 8 as a general summarization of the proposed EbHFT technique in compared with some other available approaches [13,18,19,22,25].

Owing to rational comparison, the measured performance metrics are employed to the same image dataset. Recalling the above mentioned results, the blind medical image watermarking scheme proposed in [13] utilize a hybrid DWT along with SVD. The proposed EbHFT involves the privileges of both DWT and DCT while techniques presented in [18,25] rely solely on the standard DWT. However, the Fast Discrete Curvelet Transform and Discrete Cosine Transform FDCuT-DCT were fused in [21,24]. Moving to the embedding and extraction operation, the technique introduced in [18] used three PN Sequence whilst two PN Sequence are utilized in [19]. In [22], two WGN sequence are used whereas EbHFT employs three PN sequences.

In terms of visual quality, maximum PSNR value recorded was 31.17 dB, 39.03 dB, 37.75, 52.76, and 60.84 dB for [13,18,19,22,25] respectively. Nevertheless, the proposed EbHFT achieves

57.65 dB. The maximum NC are reported in Tab. 3 for the different existing techniques with values of 0.6676, 0.7409, 0.7544 for [13,18,19]. Yet, a maximum NC value of 1 is given from [22,25] which implies full recovery of the watermark. The execution time is 7.88 seconds in the EbDT [25] and 4.96 in the proposed technique. In conclusion, the EbHFT technique succeeds in terms of perceptual quality, robustness and security when tested and compared with the other existing systems.

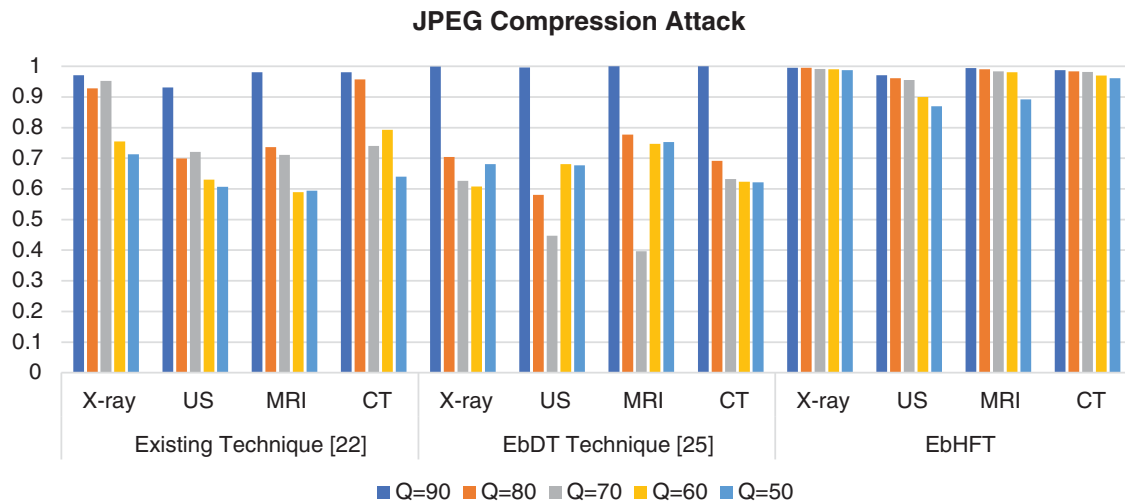


Figure 6: NC value of proposed EbHFT technique and an existing technique [22] under JPEG compression attack

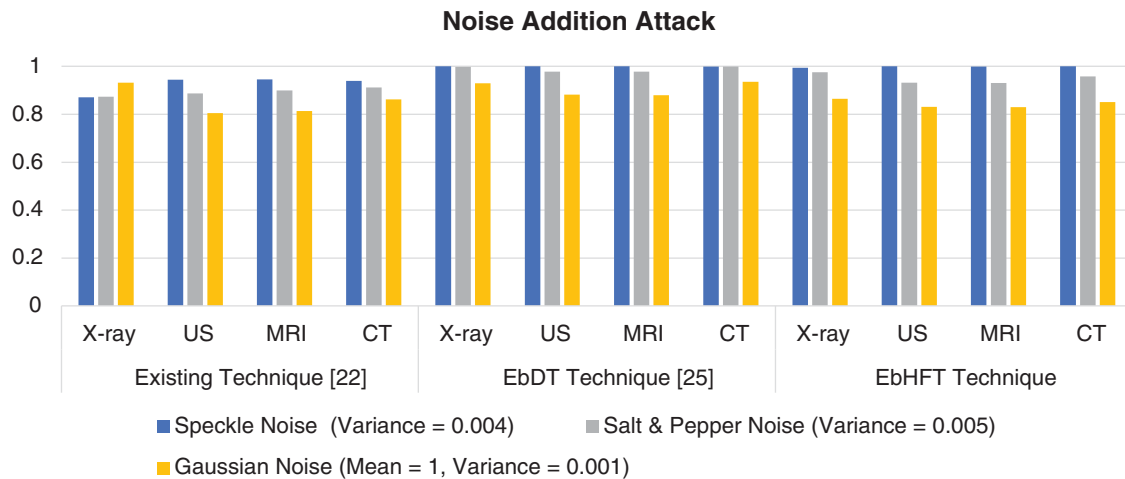


Figure 7: NC value of proposed technique and an existing technique [25] under noise addition attack

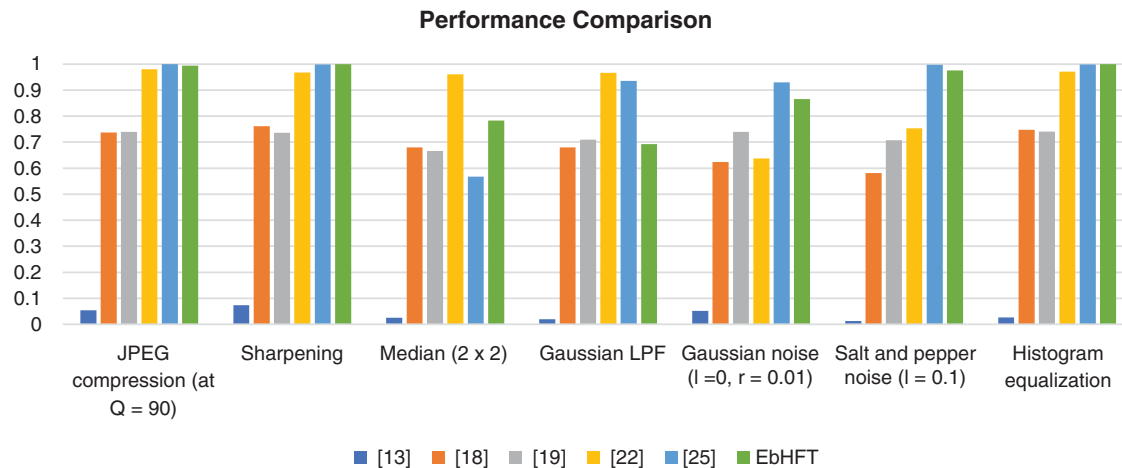


Figure 8: Performance comparison of proposed EbHFT technique with existing techniques [13,18,19,22,25] for X-ray medical images under various watermarking attacks

6 Conclusions

The study reported in this work proposed a triple-layer encryption-based strategy for safeguarding the integrity of digital images with a focus on applications in medical imaging and health informatics. Our proposed encryption-based discrete transform (EbHFT) technique fuses of Discrete Wavelet Transform (DWT) with Discrete Cosine Transform (DCT). The mid-band frequency DCT coefficients and the LL2 wavelet sub-band of the medical image are modified using three PN sequences in such a way that blind and secure extraction of watermark bit is accomplished unimpeded at the detector side. The proposed technique is tested for various medical images such as X-ray, US, MRI, and CT and compared with the performance of a similar techniques.

Furthermore, the results prove that the proposed technique outperformed the existing techniques in terms of imperceptibility, robustness, and security. The average PSNR value is above 57 dB, and the NC value is around 1 for all types of watermarked medical images based on the proposed technique. This technique is suitable for medical image protection in telemedicine applications. Notwithstanding its promising performance, the proposed strategy suffers from the poor recovery of watermark images under certain attacks such as median filter attack. As well, the strategy works only with binary watermark images. These shortenings will be addressed in the ongoing and future work.

Funding Statement: The authors received no specific funding for this study.

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

References

- [1] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, 2nd ed., Amsterdam, Netherlands: Elsevier, pp. 15–31, 2008.
- [2] G. C. Langelaar, I. Setyawan and R. L. Lagendijk, “Watermarking digital image and video data. A state-of-the-art overview,” *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, 2000.

- [3] A. Al-Haj, "Combined DWT-DCT digital image watermarking," *Journal of Computer Science*, vol. 3, no. 9, pp. 740–746, 2007.
- [4] V. M. Potdar, S. Han and E. Chang, "A survey of digital image watermarking techniques," in *Proc. of the IEEE Int. Conf. on Industrial Informatics*, Perth, Australia, pp. 709–716, 2005.
- [5] A. M. Iliyasu, A. K. Al-Asmari, A. S. Salama, M. A. Al-Qodah, M. A. Abd Elwahab *et al.*, "A Visual complexity-sensitive DWT ordering Scheme for Hiding Data in Images," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 7, no. 16, pp. 3286–3297, 2014.
- [6] K. R. Rao and P. Yip, *Discrete Cosine Transform: Algorithms, Advantages, Applications*. San Diego, CA, United States: Academic Press Professional, pp. 12–21, 1990.
- [7] A. Ali, W. Dong and L. Renfa, "A novel ZCS-clipping precoding technique for PAPR reduction using DCT-OFDM in vehicular channels," *International Journal of Hybrid Information Technology*, vol. 8, no. 5, pp. 11–22, 2015.
- [8] A. Ali, W. Dong, L. Renfa and E. Eldesouky, "ISI and PAPR immune IEEE 802.11 p channels based on single-carrier frequency domain equalizer," *KSII Transactions on Internet & Information System*, vol. 10, no. 11, pp. 5513–5529, 2016.
- [9] D. Neeta, K. Snehal and D. Jacobs, "Implementation of LSB steganography and its evaluation for various bits," in *1st Int. Conf. on Digital Information Management*, Bangalore, India, pp. 173–178, 2006.
- [10] M. Ebrahim and C. W. Chong, "Secure Force: A Low-Complexity Cryptographic Algorithm for Wireless Sensor Network (WSN)," in *IEEE Int. Conf. on Control System, Computing and Engineering*, Mindeb, Malaysia, pp. 557–562, 2013.
- [11] A. S. Salama and M. A. Mokhtar, "Combined Technique for Improving Digital Image Watermarking," in *2nd IEEE Int. Conf. on Computer and Communications*, Chengdu, China, pp. 557–562, 2016.
- [12] S. Nagpal, S. Bhushan and M. Mahajan, "An enhanced digital image watermarking technique for medical images using neural network, DWT and RSA," *International Journal of Modern Education and Computer Science*, vol. 8, no. 4, pp. 46–56, 2016.
- [13] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Springer Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3669–3697, 2017.
- [14] P. Kishore, M. Rao, C. Prasad and D. Kumar, "Medical image watermarking: Run through review," *ARPN Journal of Engineering and Applied Science*, vol. 11, no. 5, pp. 2882–2899, 2016.
- [15] A. K. Singh, M. Dave and A. Mohan, "Hybrid technique for robust and imperceptible dual watermarking using error correcting codes for application in telemedicine," *International Journal Electronic Security and Digital Forensics*, vol. 6, no. 4, pp. 285–305, 2014.
- [16] D. Biswas, P. Das, P. Maji, N. Dey and S. S. Chaudhuri, "Visible watermarking within the region of non-interest of medical images based on fuzzy c-means and Harris corner detection," in *4th Int. Workshop Communications Security & Information Assurance*, Delhi, India. Springer, pp. 161–168, 2013.
- [17] S. Chakraborty, S. Samanta, D. Biswas, N. Dey and S. S. Chaudhuri, "Particle swarm optimization-based parameter optimization technique in medical information hiding," in *IEEE Int. Conf. on Computational Intelligence and Computing Research*, Enathi, India, pp. 1–6, 2013.
- [18] A. K. Singh, B. Kumar, M. Dave and A. Mohan, "Multiple watermarking on medical images using selective discrete wavelet transform coefficients," *Journal of Medical Imaging and Health Informatics*, vol. 5, no. 3, pp. 1–8, 2015.
- [19] C. Zhang, L. L. Cheng, Z. Qiu and L. Cheng, "Multipurpose watermarking based on multiscale curvelet transform," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 611–619, 2008.
- [20] J. Xu, H. Pang and J. Zhao, "Digital image watermarking algorithm based on fast curvelet transform," *Journal of Software Engineering and Applications*, vol. 3, no. 10, pp. 939–943, 2010.
- [21] M. Bazargani, H. Ebrahimi and R. Dianat, "Digital image watermarking in wavelet, contourlet and curvelet domains," *Journal of Basic and Applied Scientific Research*, vol. 2, no. 11, pp. 11296–11308, 2012.

- [22] R. Thanki, S. Borra, V. Dwivedi and K. Borisagar, "An efficient medical image watermarking scheme based on FDCuT-DCT," *Engineering Science and Technology, an International Journal*, vol. 20, no. 4, pp. 1366–1379, 2017.
- [23] R. Eswaraiyah and E. Sreenivasa Reddy, "Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI," *International Journal of Telemedicine and Applications*, vol. 2014, no. 50, pp. 1–10, 2014.
- [24] A. K. Singh, "Some new techniques of improved wavelet domain watermarking for medical images." India: NIT Kurukshetra, Ph.D. dissertation, 2018.
- [25] A. S. Salama, M. A. Mokhtar and M. B. Tayel, "A triple-layer encryption-based watermarking technique for improving security of medical images," *Journal of Medical Imaging and Health Informatics*, vol. 9, no. 3, pp. 610–619, 2019.
- [26] A. Ali and E. Eldesouky, "Controlling high PAPR in vehicular OFDM-MIMO using downlink optimization model under DCT transform," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 11, pp. 271–278, 2019.
- [27] A. Messaoudi, F. Benchabane and K. Srairi, "DCT-based color image compression algorithm using adaptive block scanning," *Signal, Image and Video Processing*, vol. 13, no. 7, pp. 1441–1449, 2019.
- [28] A. Salama, R. Atta, R. Rizk and F. Wanes, "A robust digital image watermarking technique based on wavelet transform," in *IEEE Int. Conf. on System Engineering and Technology*, Shah Alam, Malaysia, pp. 100–104, 2011.
- [29] M. Saha, M. K. Naskar and B. N. Chatterji, "Advanced wavelet transform for image Processing—A survey," *Information, Photonics and Communication*, vol. 79, pp. 185–194, 2020.
- [30] A. K. Al-Asmari, A. Salama, A. M. Iliyasu and M. A. Al-Qodah, "A DWT ordering technique for hiding data in images using pixel value difference," in *IEEE Eighth Int. Conf. on Computational Intelligence and Security*, Guangzhou, China, pp. 553–557, 2012.
- [31] P. Meerwald and A. Uhl, "A Survey of wavelet-domain watermarking algorithms," in *Proc. of the SPIE Security and Watermarking of Multimedia Contents III, Photonics West 2001-Electronic Imaging*, San Jose, CA, United States, vol. 4314, pp. 505–516, 2001.
- [32] A. S. Salama, M. A. Al-Qodah, A. M. Iliyasu, A. K. Al-Asmari and F. Yan, "A hybrid fusion technique for watermarking digital images," *Advances in Intelligent Systems and Computing*, vol. 240, pp. 207–217, 2014.
- [33] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [34] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [35] MedPix™ Medical Image Database MedPix is registered Trademark of USUHS. 2020. [Online]. Available: <http://rad.usuhs.mil/medpix/medpix.html>, <https://medpix.nlm.nih.gov/home>.