



## A Robust Medical Images Watermarking Using FDCuT-DCT-SVD

Ledy Novamizanti<sup>1\*</sup>    Ida Wahidah<sup>1</sup>    Ni Putu Dhea Prameiswari Wardana<sup>1</sup>

<sup>1</sup>*School of Electrical Engineering, Telkom University, Bandung, Indonesia*

\* Corresponding author's Email: ledyaldn@telkomuniversity.ac.id

---

**Abstract:** One way to prevent image duplication is by applying watermarking techniques. In this work, the watermarking process is applied to medical images using the Fast Discrete Curvelet Transforms (FDCuT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD) methods. The medical image of the host is transformed using FDCuT so that three subbands are obtained. High Frequency (HF) subband selected for DCT and SVD applications. Meanwhile, SVD was also applied to the watermark image. The singular value on the host image is exchanged with the singular value on the watermark. Insertion of tears by exchanging singular values does not cause the quality of medical images to decrease significantly. The experimental results prove that the proposed FDCuT-DCT-SVD algorithm produces good imperceptibility. The proposed algorithm is also resistant to various types of attacks, including JPEG compression, noise enhancement attacks, filtering attacks, and other common attacks.

**Keywords:** Discrete cosine transform, Fast discrete curvelet transforms, Medical image, Singular value decomposition, Watermarking.

---

### 1. Introduction

Human needs are constantly increasing, causing information technology to grow. The development of information technology has an impact on the editing process, distribution, and production of digital multimedia in a personal way that becomes easy and fast. Illegal duplication is one of the effects of this convenience [1]. The development of various remote medical services, such as teleconsultation, telemedicine, teleradiology, and teleradiology, has made electronic medical record management increasingly popular. The main priority in handling medical images is to protect patient documents from all acts of damage done by unauthorized parties [2]. Therefore, it is necessary to do a digital watermarking process. Digital watermarking is a powerful method of guaranteeing the information isn't circulated illicitly, and it's being utilized adequately to stop the acts of neglect [3].

One solution for protecting a patient's medical image is the watermarking technique. Digital watermarking is a method of insertion of information (watermark) object to the host so that the watermark

data can only be detected by a person who is given the authority. Watermarking on medical images cannot be done arbitrarily and must heed two things. First, the watermarking procedure must not interfere with the quality of the medical image. Second, patient confidential information embedded in watermarked images must be easily retrieved without the risk of error after extraction [2].

N. Rathi and G. Holi [4] suggested that the Discrete Wavelet Transform (DWT) method can be replaced with DCT to increase the robustness of the watermark. In addition, R. Thanki [5] states FDCuT can offer better imperceptibility when compared to other methods. The DCT method was chosen because this method can give a good perception of invisibility and robustness. The SVD method is very stable. When the image contains little information, the singular value does not change drastically.

This study proposes a medical image watermarking scheme using the FDCuT, DCT, and SVD method. The strong point of this approach is that the watermark insertion is located in the HF subband of the host image that has received FDCuT. The HF subband can produce better imperceptibility than

other subbands. The SVD on FDCuT+DCT-based image hosts increase imperceptibility and robustness. We arrange the next section of the paper as follows. Section 2 discusses various academic articles on medical image watermarking. Section 3 briefly describes the watermarking method used in this study. Section 4 provides a description of the proposed algorithm, which includes the embedding and extracting processes. Section 5 discusses the experiment result of the proposed scheme, which includes imperceptibility and robustness. Then the performance of the proposed algorithm is compared with other recent algorithms. Furthermore, Section 6 reports the conclusions and proposals for future research.

## 2. Literature review

Watermarking system with multiple watermarks is used to help solve various problems such as high protection of medical images for patient safety and resistance to various attacks [6]. N. Mohananthini and G. Yamuna stated that the watermark's blue part achieves more robustness in separating channels and fusing the watermarking algorithm as opposed to the watermark's red and green part. The watermarking algorithms based on DWT and SVD achieve imperceptibility, robustness against attacks. But then, there is no explanation of why CT medical imagery can provide a better imperceptibility compared to MRI and X-ray. S. D. Mashalkar and S. S. Shirgan [7] applied two digital watermarking methods for patients privacy or copyright rights of MRI images. It is observed from the analysis that both methods are appropriate for watermarking. It can be seen from tests that the derived for the SVD method is clearer than the DWT method. However, the type of medical image used is not varied. This study only uses MRI image. So there is no comparison of results with other types. S. Ajili, M. A. Hajjaji, and A. Mtibaa [8] used a combining SVD and DWT scheme for integrating patient's data in medical images. The findings of the experiment show greater robustness of the proposed scheme against many forms of attacks. The robustness is achieved by means of the serial turbo code to enhance the protection of the inserted message (watermark) against attacks, SHA-1 hash function, DWT space, and SVD to boost the watermark integrity. But then, the host used in this research are not varied, only using MRI images. S. Gajula and V. Rajesh [9] suggested a watermarking image scheme using DWT and SVD techniques using uniform distribution function as a scaling factor. The obtained results are very helpful for the integrity of medical images. The technique provides a better

response to medical images. However, the only quality measures used are PSNR and MSE.

An SVD based fragile watermarking scheme was investigated by A. Shehab et al. [10]. The study proposed a clustered block method, thus providing an efficient way to locate the affected block areas in different medical images. The scheme also provides more security and very accurate. The proposed scheme effectively prevents VQ attacks, content deletion, copy and paste attacks, and text adds attacks. Compared to the cutting edge approach, the proposed scheme greatly improves the accuracy of tamper localization and the quality of self-restored images. However, there are still other attacks that greatly change the medical image after the watermark is inserted, such as cropping, flipping, rotate, attacks in this study are still limited. I. Assini et al. [11] employed the DWT-DCT-SVD hybrid watermarking technique to ensure copyright rights and medical image security. DWT provides better identification based on the characteristics of the Human Visual System (HVS). Then, the DCT produces the perception of toughness and good sharpness. In addition, when small information is added to the image, the singular value in the SVD is very stable. The singular value doesn't change drastically. However, the scheme only tests additional noise and filtering attacks.

H. U. Seo et al. [12] proposed a medical image watermarking algorithm using a bit just noticeable distortion -based threshold map in DCT methods. This technique was defined for the embedding and extraction of a watermark based on the DC coefficients in the DCT low-frequency region. As the low frequency comprises most energy of the original image, the image quality is crucially affected. The watermark is immediately included in the DC coefficient. This impacts significantly on robustness and image quality. It also offers excellent invisibility, as it takes HV into account when embedding the watermark. The findings suggest that the method proposed is robust against a number of attacks. The drawback of this work is that the PSNR value is small, not reaching 50 dB. H. Ayad and M. Khalil [13] presents a new semi-blind watermarking image method for medical applications. The proposed scheme is based on a combination of DWT and SVD to transparently embed the watermark and remove it with great fidelity. The QAM-16 has also been used to encode and insert text characters into the host image. Overall, the proposed scheme shows a good interaction between imperceptibility, robustness, and capacity in relation to the state of the art methods. The experimental results show the efficacy of integrating wavelet algorithm with SVD technique in

terms of imperceptibility compared with non-hybrid SVD or DWT methods. The limitation of this research is that the attacks carried out do not vary, so it is not known whether the secret key can still be used for the watermark image that has undergone this change.

M. Al-qdah [14] was proposing a hybrid watermarking technique for medical imaging. The study uses a combination of three transforms: DWT-DCT-SVD. Such limited study findings indicate that watermarking of medical images with a watermark of specific patient information does not impact the visual appearance of the initial medical images significantly, and they can be utilized for medical purposes. It was experimentally quantitatively demonstrated using the HVS metrics that the watermarked medical images were similar to their originals. Also, choosing the appropriate watermarking algorithm is essential to obtain the robustness, imperceptibility, and security needed to protect the patients' personal data inside a medical image. The drawback of this work is that after watermarking medical images or even after hitting the images, the algorithm can't determine how much medical information is lost. N. Rathi and G. Holi [4] applied DCT to the DWT-SVD blind watermarking technique. Then the performance of the two schemes is compared. Tests for the respective techniques are being evaluated. It was found that the watermarking algorithm based on DWT-DCT-SVD is robust as compared to the DWT-SVD process. This system can be used for authentication purposes and to hide data. The limitation of existed DWT-DCT-SVD method, there is a rapid degradation between Normalized Correlation without attacks compared to when given an attack. So that additional method are needed or substitute for one of the methods used. A. Mehto and N. Mehra [15] applied DWT and DCT to produce digital image watermarking that is secure, robust, and without loss. The experimental findings demonstrate the feasibility of the proposed scheme. The high imperceptibility represents that the image quality is not degraded and provides good visualization. There is no attack is a drawback of this study, while in the abstract it is stated that the scheme to be made is robust. S. Borra and R. Thanki [16] applied Compressive Sensing with DCT to produce a non-blind and fragile watermarking technique. The watermark is a biometric image that is hidden in the radiological image of the patient. The application of these techniques increases the reliability of cover medical image in the teleradiology model at various safety points. Compared to the current medical image detection scheme, the efficiency of the proposed scheme has better imperceptibility and more potential

for payload. However, the SSIM value decreased dramatically when the watermarked image was attacked. U. Verma and N. Sharma [17] compared the hybrid techniques DWT + SVD, with other medical image watermarking techniques. Based on the findings, this SVD has consistent SSIM performance for all attacks. Thus, DWT and SVD hybrid technique is implemented in medical image watermarking to combine the benefits of both techniques. Combined techniques produce better and more consistent performance than individual techniques. The limitation of this study is that when given an attack, the CRC and SSIM values are far from ideal. With the naked eye, indirect images can be recognized. N. Venkatram et al. [18] proposed Lifting Wavelet Transform and SVD for watermarking different medical image forms such as MRI, CT, and US. After attacks, the results show this method gives satisfactory quality both mathematically and visually. But then, the NC value when given an attack is below 0.7. B. Madhu and G. Holi [19] applied a combination of Stationary Wavelet Transform and SVD at HH sub-band. The method proposed is robust and has the ability to counteract numerous attacks that cause information loss. Compared to the previous method in this paper, it is seen that the increase was more in terms of the PSNR value, while for dominant NC it decreased.

A blind watermarking scheme based on FDCuT and DCT was investigated by R. Thanki et al. [5]. The proposed scheme was tested with several medical images, including MRI, CT, X-ray, and AS. Then, the results obtained are compared with the results of the current scheme. The proposed scheme worked better in terms of robustness, imperceptibility, and security than current schemes. However, the extracted watermark image continuously presents noise. R. M. Thanki et al. [20] is proposing a hybrid non-blind watermarking technique based on FDCuT and DCT. This technique is vulnerable to various watermarking attacks and offers more ability in relation to existing watermarking techniques in the literature. The technique proposed also provides authentication of the biometric image in the multi-biometric device's system database. This does not weaken the multibiometric system's verification and authentication efficiency. The drawback of this technique is that for the extraction of watermark fingerprint image on the extraction side, DCT base matrix and correct measuring matrix are needed. S. H. Soleymani et al. [21] proposed a robust and blind watermarking system that is highly resistant to popular image watermarking attacks, including noise, compression, and processing of image quality improvements. The position of embedding in this

approach is the high-frequency coefficients of the FDCuT transform approximation sub-band. However, the difference imperceptibility between watermarked images using Arnold Cat and watermarked images without Arnold Cat is tiny. The proposed algorithm uses the FDCuT-DCT-SVD approach to increase the robustness and imperceptibility of traditional algorithms.

### 3. Preliminaries

#### 3.1 Fast discrete curvelet transforms

Discrete Time Curvelet Transforms (DTCuT) is used for images in order to achieve various sub-band frequencies [5]. DTCuT applies image processing by representing an image into curves or edges. DTCuT is linear and becomes a Cartesian array input of shapes  $f[t_1, t_2]$ ,  $0 \leq t_1, t_2 < n$ , enabling output as a set of coefficients as seen in the Eq. (1).

$$C^D(i, j, k) := \sum_{0 \leq t_1, t_2 \leq n} f[t_1, t_2] \overline{\varphi_{i,j,k}^D[t_1, t_2]} \quad (1)$$

with every  $C^D(i, j, k)$  is a curvelet digital waveform ( $D$  is an abbreviation of Digital,  $i$  and  $j$  are scale parameter and orientation parameter, respectively, with  $i=j=0, 1, 2, \dots$ ; and  $k=(k_1, k_2) \in \mathbb{Z}^2$  is a translation parameter. The scale parameters depend on the image size and can be determined using  $\log_2(\min(M, N) - 3)$ , with  $M, N$  is the image row and column size. The orientation parameter must be a multiple of four, and the orientation parameter defaults to 16 [5].

DTCuT has been redesigned with a new mathematical architecture that is simple and easy to implement. This design is known as Fast DTCuT (FDCuT). Curvelet transformations are divided into two types. The first is FDCuT based on Unequally-Spaced Fast Fourier Transforms (USFFT). Second is the frequency wrapper based FDCuT. USFFT-based FDCuTs have unequal and complex sample sizes and also require more computation time. Meanwhile, frequency wrapper based FDCuT is easier to understand and use. Besides that, frequency wrapping computation time based FDCuT is faster than USFFT based FDCuT, so many researchers choose it.

#### 3.2 Discrete cosine transform

DCT is a technique applied to spatial domain image pixels to transform them into a frequency domain where redundancy can be defined [22]. In the DCT, the image energy is concentrated into coefficients in small quantities, so that more energy-dense. Then DCT can minimize interdependence in

coefficients. The image is divided into  $8 \times 8$  blocks in JPEG compression, and then a 2-D DCT is applied to each of those  $8 \times 8$  blocks. The Inverse Discrete Cosine Transform (IDCT) is applied in JPEG decompression to the  $8 \times 8$  DCT coefficient block. DCT can be seen in Eq. (2) and IDCT can be seen in Eq. (3).

$$F(u, v) = \frac{1}{4} C(u) C(v) \sum_{i=0}^7 \sum_{j=0}^7 f(i, j) \cos\left(\frac{(2i+1)u\pi}{16}\right) \cos\left(\frac{(2j+1)v\pi}{16}\right) \quad (2)$$

$$f(i, j) = \frac{1}{4} \sum_{u=0}^7 \sum_{v=0}^7 C(u) C(v) F(u, v) \cos\left(\frac{(2i+1)u\pi}{16}\right) \cos\left(\frac{(2j+1)v\pi}{16}\right) \quad (3)$$

with  $f(i, j)$  is the value of each pixel, and  $F(u, v)$  is the DCT coefficient. While  $C$  is calculated by Eq. (4).

$$C(\omega) = \begin{cases} \frac{1}{\sqrt{2}}, & \omega = 0 \\ 1, & \omega = 1, 2, \dots, 7 \end{cases} \quad (4)$$

#### 3.3 Singular value decomposition

SVD is a factoring matrix by breaking down a matrix into three-unit matrices, namely  $U$ ,  $V$ , and a diagonal matrix  $S$  containing a scale factor called the singular value [23]. Some applications that utilize SVD are in the fields of signal processing and statistics. SVD can be seen as a generalization of a changing spectral theorem. It does not have to be always square, and in the form of a matrix. The spectral theorem states that normal matrices can be diagonalized, that is represented as diagonal matrices on several bases. SVD is a numerical analysis technique in digitizing a matrix. This technique is now used in inserting watermarks into an image. This technique is a newer technique when compared to DCT.

Suppose there is an image of size  $M \times N$  that will be watermarked. The image can be presented in a nonzero matrix and made into Eq. (5).

$$A = USV^T \quad (5)$$

with  $A$  is the matrix of images sized  $M \times N$ ,  $U$  is orthogonal matrix sized  $M \times M$ ,  $S$  is singular matrix sized  $M \times N$ , and  $V$  is orthogonal matrix sized  $N \times N$ . The benefit of using the SVD technique is that the image's  $SV$  is constant, that is, even if the image changes slightly, the image's  $SV$  will not be affected. Another advantage is that there is no limit on the size of the matrix; the matrix can be square or rectangular [24].

#### 4. Proposed watermarking model

Fig. 1 is a medical image watermarking in general. Firstly, in the embedding process, the representation of a watermark is embedded in the medical image. The method of extraction is related to the extraction of a watermark image embedded in a medical image. The watermark image itself will be used for security purposes to authenticate the medical image. Fatigue images can be identified by extracting watermark images from watermarked medical images. If the extraction results from the watermark image do not match the original medical image, the recipient will know that an attack has occurred. After authentication, the receiver must examine the medical data. When a medical image is caught, the recipient discards the medical image.

##### 4.1 Watermark embedding

Fig. 2 (a) is the watermark embedding process.

1. Reads the host's medical image and watermark image.
2. FDCuT is applied to the host image.
3. Three subbands are obtained, namely, HF, MF, and LF. Take the HF part to be processed to the next stage.
4. DCT is applied to the HF subband, with the aim of dividing the host image into 8×8 pixel blocks. Furthermore, DCT also refers to watermarking images and divided into 8×8 pixel blocks.
5. SVD is used on blocks placed prior to DCT. In the host image, obtained  $U$ ,  $S$ , and  $V$  matrix.  $U$  (orthogonal matrix size  $M \times M$ ),  $S$  (singular matrix size  $M \times N$ ), and  $V$  (orthogonal matrix size  $N \times N$ ). Meanwhile, the watermark image is obtained  $U_w$ ,  $S_w$ , and  $V_w$ .

$$I = U \times S \times V \quad (6)$$

$$W = U_w \times S_w \times V_w \quad (7)$$

6. Exchange the diagonal matrix  $S$  with the diagonal matrix  $S_w$ .

$$I_{wat} = U \times S_{wm} \times V^T \quad (8)$$

7. Apply Invers SVD (ISVD) to  $I_{wat}$ .
8. Apply IDCT and Inverse FDCuT (IFDCuT). The end result of this embedding process is a medical image that has been inserted watermark.

##### 4.2 Watermark extracting

Fig. 2 (b) is the watermark extracting process.

1. Read watermarked and watermark images.
2. FDCuT is applied to the watermarked image.
3. DCT is applied to the HF subband of FDCuT so that the image is divided into 8×8 pixels.
4. The SVD method is applied to get the  $S_{ew}$  or diagonal matrix of the watermarked image.
5. Apply SVD to the original watermark image, to obtain  $U_w$ ,  $S_w$ , and  $V_w$ .

$$I_w = U_{ew} \times S_{ew} \times V_{ew} \quad (9)$$

$$W = U_w \times S_w \times V_w \quad (10)$$

6. Apply the ISVD to  $U_w$ ,  $V_w$  from the original watermark, and  $S_{ew}$  from the watermarked image. The final result is the extracted watermark image.

$$W' = U_w \times S_{ew} \times V_w^T \quad (11)$$

#### 5. Results and discussion

The designed system is tested with specific types of medical images, including: CT, MRI, US, and X-rays. Each type of medical image has three images, so the total host image used is nine images. Medical images obtained from the MedPixTM database. The medical image size used is 1024×1024 pixels, with an 8-bit gray image type. Fig. 3 represents the binary watermark we used. Watermark image size is 128×128 pixels with binary image type.

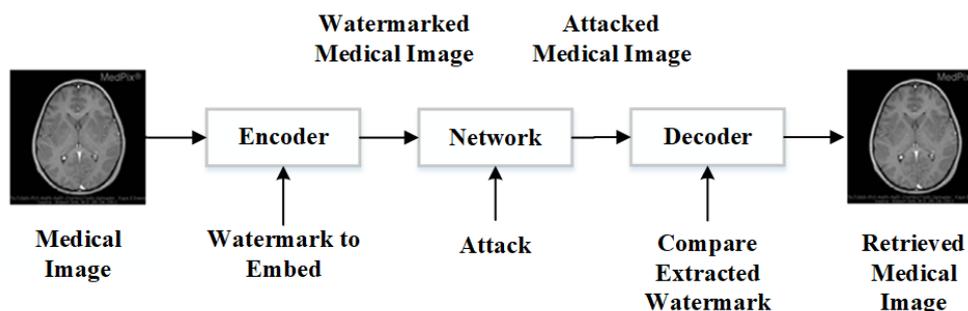


Figure. 1 Medical image watermarking in general

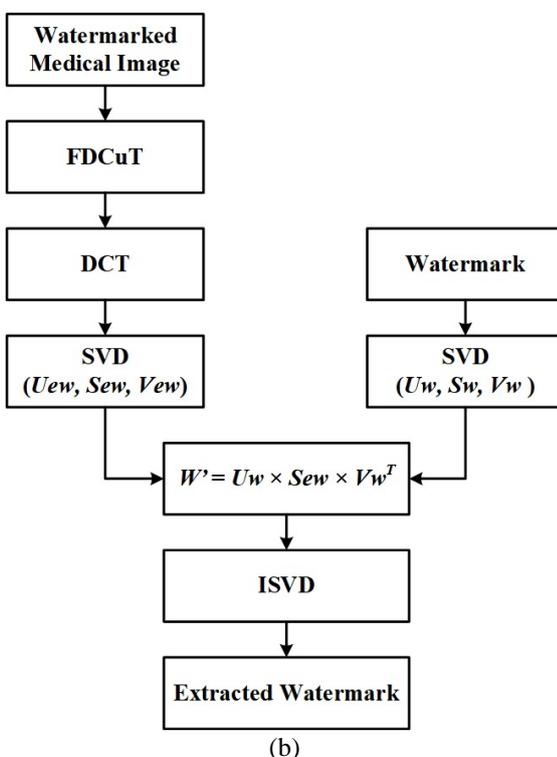
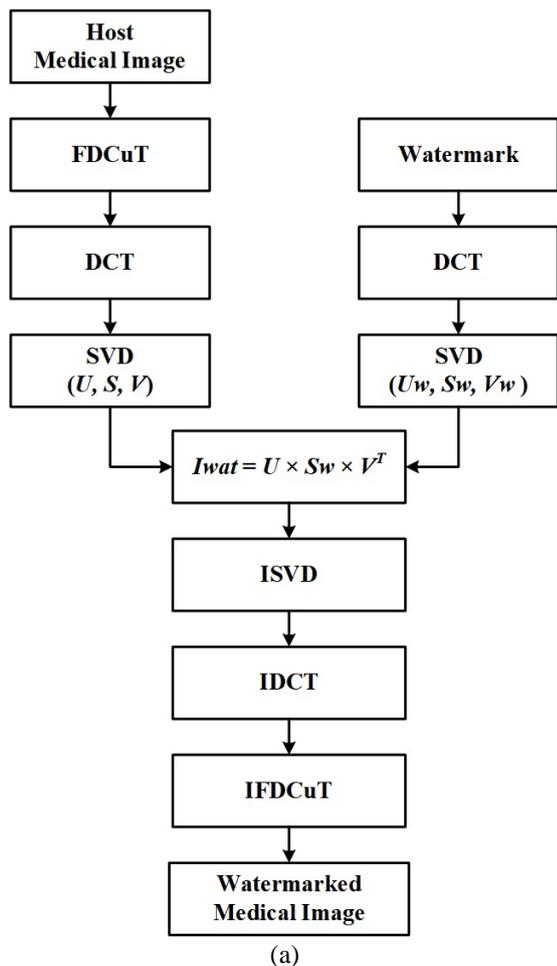


Figure. 2 Watermark process: (a) embedding and (b) extracting



Figure. 3 Binary watermark

Two universal metrics are used for objective evaluation, namely Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM). PSNR is used to calculate imperceptibility between the original host image and the new image with a watermark. The PSNR value in dB units can be obtained from the calculation of Eq. (12). PSNR is the ratio between the maximum value of the bit depth of the image with the amount of noise that affects the measured signal. For an 8 bit image, the maximum value is 255. The noise value is represented by the Minimum Square Error (MSE). The MSE formula is obtained by Eq. (13). A weak PSNR value suggests more unsightly algorithms.

$$PSNR_{(dB)} = 10 \times \log_{10} \left( \frac{255^2}{\sqrt{MSE}} \right) \quad (12)$$

$$MSE = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (C(x, y) - CW(x, y))^2 \quad (13)$$

SSIM is used to measure the similarity of two images. The purpose of SSIM is to obtain the similarity value between the extracted watermark image and the original watermark image before the insertion process. SSIM can be calculated through the Eq. (14):

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (14)$$

with  $\mu_x$  and  $\mu_y$  are the mean of the  $X$  and  $Y$  images,  $\sigma_{xy}$  represents the covariance of the  $X$  image against  $Y$ ,  $\sigma_x^2$  represents the variant of the  $X$  image,  $\sigma_y^2$  represents the variant of the  $Y$  image,  $C_1$  is  $(k1L)^2$  and  $C_2$  is  $(k2L)^2$  where  $L$  is the image range (2bit - 1) with default values  $k1 = 0.01$  and  $k2 = 0.03$ . SSIM value, which is between 0 to 1. If the calculation results get closer to 1 then it can be said that the decompression image is exactly the same as the original image and has better image quality.

For all tested images, different attacks have been applied, and the watermark is extracted with different qualities. First, the watermarked image is extracted without being subjected to any attacks. Then, the watermark is extracted after applying different attacks. The results of applying these attacks on the extracted watermark are assessed using two metrics,

the Normalized Correlation (NC) and the Bit Error Rate (BER). NC parameter is used for watermarking robustness measurements. The NC formula using Eq. (15).

$$NC = \frac{\sum_{x=1}^N \sum_{y=1}^M w(x,y) \times w'(x,y)}{\sum_{x=1}^N \sum_{y=1}^M w^2(x,y)} \quad (15)$$

NC assesses the similarity between the original and the extracted watermark. When the NC value exceeds one, is said to be robust watermarking scheme. BER is calculated using Eq. (16):

$$BER = \frac{1}{m \times n} \sum_i^m \sum_j^n [w_{ij} \otimes w'_{ij}] \quad (16)$$

with  $w$  and  $w'$  are original and recovered watermark, respectively each of size  $m \times n$  [25]. Twelve different images were used to embed the binary watermark.

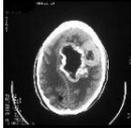
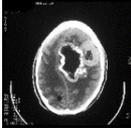
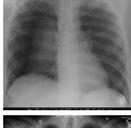
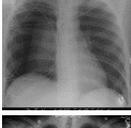
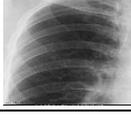
This study analyzes the performance of several experiments, namely imperceptibility and robustness tests using various medical images. The efficiency of a watermarking algorithm is largely determined by the perceptual quality of the watermarked images and the watermark's robustness. The output measurements can be calculated using PSNR between the host and the watermarked medical image. This test is conducted to verify whether deterioration occurs in the medical image after insertion of the watermark image in it. Table 1 displays the NC and BER for the watermark extracted after applying specific attacks. The PSNR, NC, BER, and SSIM values for the different test images are shown in Table 1. Based on the test results, the watermark image has high values for these four metrics. Table 2 shows the images tested with the watermark image results. The watermarked host image and the original image did not show the slightest difference. The watermarked image looks like the original image so that the watermarking scheme meets the imperceptibility criteria.

Table 1. Test results of the watermarking scheme

Image	PSNR	SSIM	NC	BER
CT 1	54.0226	0.9915	0.7968	0.0486
CT 2	53.7124	0.9915	0.8995	0.0308
CT 3	53.8859	0.9980	0.8704	0.0411
MRI 1	54.2478	0.9973	0.6218	0.1313
MRI 2	53.8619	0.9919	0.9202	0.0228
MRI 3	53.4559	0.9948	0.9579	0.0100
US 1	55.0535	0.9945	0.6564	0.1021
US 2	53.7620	0.9974	0.9258	0.0197
US 3	55.3963	0.9930	0.6681	0.1063
X-ray_1	53.5433	0.9958	0.9441	0.0172

X-ray_2	53.8006	0.9966	0.9172	0.0203
X-ray_3	53.6303	0.9968	0.9479	0.0141

Table 2. The original and watermarked image results

Image	Medical Images	Watermarked Images
CT 1		
CT 2		
CT 3		
MRI 1		
MRI 2		
MRI 3		
US 1		
US 2		
US 3		
X-ray_1		
X-ray_2		
X-ray_3		

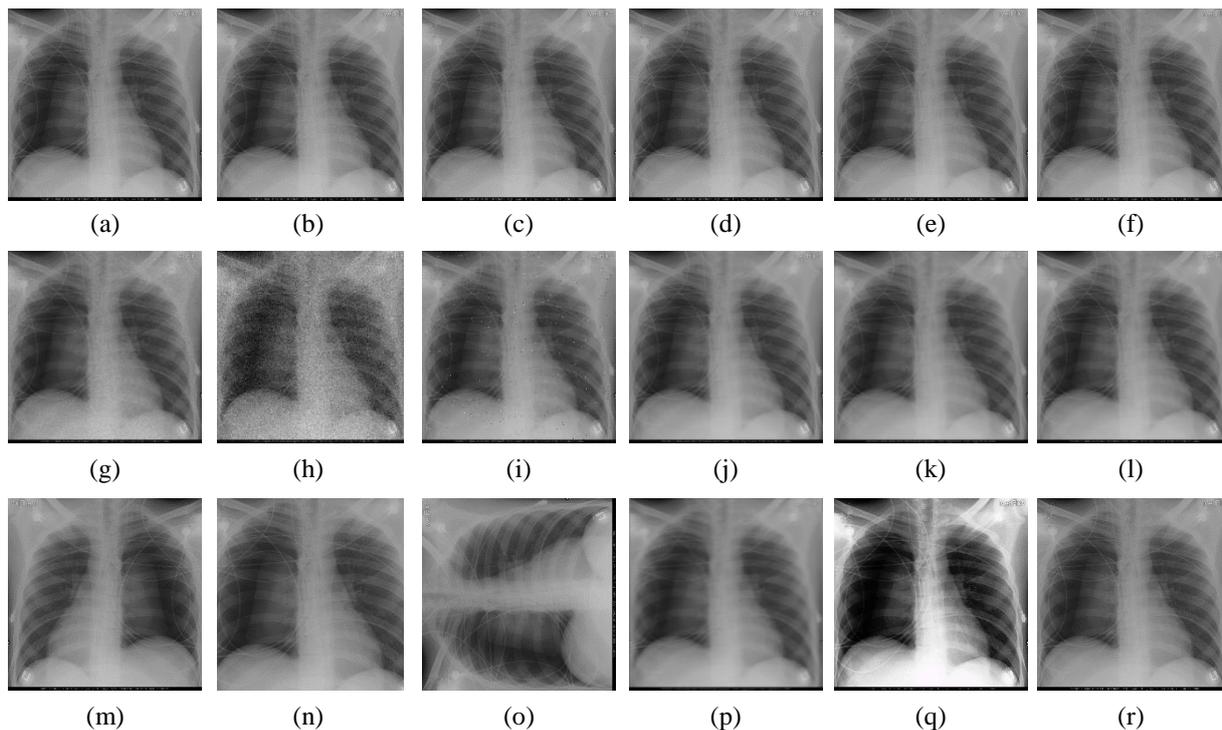


Figure. 4 Display one medical image given attack: (a) no attack, (b)-(f) JPEG compression attack with qualities (Q) respectively 50, 60, 70, 80, and 90, (g)-(i) noise addition respectively speckle, Gaussian, and salt & pepper noise, (j)-(l) filtering attacks respectively median filtering, mean filtering, and Gaussian LPF, (m)-(o) geometric attacks respectively flipping, cropping, and rotation, and (p)-(r) common attack respectively blurring, histogram equalization, and sharpening

For robustness tests, watermarked medical images are given various watermarking attacks, including JPEG compression, noise addition, filtering, geometric attacks, and multiple types of common attacks. Three types of filtering attacks, including Gaussian Low Pass Filter (LPF), mean, and median. The geometric attacks used are cropping, rotation, and flipping. While the common types of attacks are histogram equalization, blurring, and sharpening. The sample of applied attack is shown in Fig. 4. The extracted watermark after JPEG compression and noise addition attacks is shown in Table 3. The proposed watermarking system seems to be resistant to attacks but not on all forms of medical images. The extracted watermark after the JPEG compression attack tends to be resistant to attack by the proposed watermarking even if not on all forms of medical images. The NC value obtained after extraction was above 0.7, which means that the watermark image was still good and did not change much when it was extracted. The US image type has the smallest NC value, this is related to the frequency distribution of the pixel intensity value in an image. In addition, the higher the JPEG quality value given to the inundated images, the higher the NC, the smaller BER, and the extracted watermark clearly visible.

The watermarking scheme for noise addition attacks can still be extracted properly and the NC

value in this attack is categorized as good. Salt & pepper noise attacks have the best extraction results with very little difference with speckle noise attacks. When an image with a Gaussian noise attack is extracted, it can be seen that the watermark extraction image simultaneously has white spots around the logo. The extracted watermark after filtering, geometric, and various attacks are shown in Table 4. The results in the median filtering and Gaussian filtering are the same, both for NC and BER values, as well as for visualization of extraction watermarks. Mean filtering attacks produce poor watermarks. This watermarking scheme is not resistant to geometric attacks, shown from the absence of a well-extracted watermark image. In addition, the NC value approaches 0, and BER approaches 1, which means that the watermark is not acceptable. The results of various attacks displayed are good, although not for all medical images. Blurring attacks can only be applied to medical X-ray types. When extracted from a sharpening attack, NC after being extracted, approaches NC without attack. Histogram equalization attack gives the effect of a diagonal line on the extracted watermark image.

This study proposes a semi-blind medical image watermarking scheme using the FDCuT, DCT, and SVD method. The proposed method is a high level of imperceptibility and also robust. Comparisons with

Table 3. Extracted watermark after JPEG compression and noise addition attacks

Image	No Attack	JPEG compression					Noise addition attack		
		Q 50	Q 60	Q 70	Q 80	Q 90	Speckle	Salt & Pepper	Gaussian
CT 1									
CT 2									
CT 3									
MRI 1									
MRI 2									
MRI 3									
US 1									
US 2									
US 3									
X-ray_1									
X-ray_2									
X-ray_3									

previous studies are important to make the contribution to the research seem more certain. Thakkar et al. [26] applied the DWT-SVD method.

The use of error correction code provides better watermark content recovery. The proposed methods have similarities; they both use SVD. But the

Table 4. Extracted watermark after filtering, geometric attack, and various attacks

Image	Filtering attack			Geometric attack			Various attack		
	Median Filtering	Mean Filtering	Gaussian LPF	Flipping	Rotation	Cropping	Blurring	Sharpening	Histogram Equalization
CT 1									
CT 2									
CT 3									
MRI 1									
MRI 2									
MRI 3									
US 1									
US 2									
US 3									
X-ray_1									
X-ray_2									
X-ray_3									

difference, the proposed method without using error correction code.

Thakur et al. [27] using DWT-DCT-SVD in which the combination of these methods can improve the robustness. Their research used two-dimensional

Table 5. Experimental conditions of several schemes

Property	Thakkar et al. [26]	Thakur et al. [27]	Thanki et al. [5]	Proposed
Cover Image	1024×1024	512×512	1024×1024	1024×1024
Watermark	32×32	256×256	128×128	128×128
Domain	Transform	Transform	Transform	Transform
Visual Logo	Yes	Yes	Yes	Yes

Table 6. Comprehensive scheme comparison

Features	Thakkar et al. [26]	Thakur et al. [27]	Thanki et al. [5]	Proposed
No. of Image Processing Transforms	2	3	2	3
No. of Noise Sequences	Not Used	Not used	Two WGN Sequences	Not Used
Maximum PSNR (dB)	48.7972	35.5250	51.58	55.3963
Maximum NC	0.6676	0.9989	0.9918	0.9579

Table 7. NC results of various current medical image watermarking schemes against various attacks

Attacks	NC for Watermark Logo			
	Thakkar et al. [26]	Thakur et al. [27]	Thanki et al. [5]	Proposed
JPEG Compression (Q 90)	0.0543	0.9975	0.9806	0.9265
Salt & Pepper Noise ( $\mu$ 0.1)	0.0132	0.8193	0.7532	<b>0.9473</b>
Gaussian Noise ( $\mu$ 0, $\sigma$ 0.01)	0.0520	0.9144	0.6377	<b>0.9770</b>
Median (2×2)	0.0252	0.6973	0.9607	0.9570
Gaussian LPF	0.0196	not reported	0.9668	0.9570
Sharpening	0.0737	0.8943	0.9674	<b>0.9890</b>
Histogram Equalization	0.0264	0.6038	0.9708	0.8909

logistic map based chaotic encryption to improve security. The proposed method also uses three transformations, both in embedding and extracting. The difference between these two studies is that on the proposed method, the DWT is replaced with FDCuT.

R. Thanki et al. [5] proposed FDCuT + DCT to achieve high imperceptibility and robustness. The proposed method has similarities with their scheme, which is both FDCuT and DCT. The difference is replacing the mid-band frequency coefficient and two white Gaussian noise (WGN) with SVD in the watermark insertion and extraction process. Table 5 presents the experimental conditions of several schemes. Meanwhile, Tables 6 and 7 show a comparative study between the methods and results of the existing scheme and the proposed scheme.

Based on Table 6, it can be seen that the proposed method has a better PSNR than Thakkar et al. [26], Thakur et al. [27], and Thanki et al. [5]. The imperceptibility value can be better because of the use of SVD on FDCuT and DCT-based image hosts so that it can increase imperceptibility. SVD is a stable method; that is, when small information is inserted into the image, the singular value does not change significantly.

In this study, apart from the imperceptibility assessment, robustness testing was also carried out using the NC parameter. Table 6 shows the results of NC calculations for the non-attack extraction results of the scheme proposed by the previous method. While Table 7 shows the results of NC calculations for the extraction results by the attack from the scheme proposed by the previous method. Based on the results presented in Table 6, it shows that the proposed method can properly extract all watermark images that have not been attacked. However, the NC obtained on watermark extraction without attack is no better than the scheme proposed by Thakur et al. [27] and R. Thanki et al. [5]. Proposed schemes have a greater NC value in more attacks, which indicates the proposed scheme has a more robust performance. After being given the attack, the proposed method is superior to salt & pepper noise, Gaussian noise, and sharpening attacks. While the method of Thakur et al. [27] is superior only to the JPEG compression attack. The method of Thakkar et al. [26] has smaller NC and PSNR values compared to the other three schemes. R. Thanki et al. [5] excelled against median attack, Gaussian LPF, and histogram equalization. The application of SVD methods with different schemes will yield good results when inserting the watermark

image into the host image. Thus, although the proposed method is not superior in robustness without being given an attack, as in method [27], the proposed method provides an increase in the NC value of about 0.29 when compared to the method [26]. Robustness criteria are maintained during various attacks.

## 6. Conclusion

In this paper, we apply the SVD method to the medical image watermarking technique based on FDCuT-DCT. The proposed algorithm has good imperceptibility so that it can maintain the quality of medical images. In this paper, the system performance is reported using the PSNR, SSIM, BER, and NC parameters. By applying the semi-blind watermarking technique, the maximum PSNR value 55.3963 dB, SSIM maximum 0.9980, NC maximum 0.9579, and BER 0.01. This watermarking scheme is resistant to noise addition attacks, JPEG compression, filtering attacks, and various common attacks.

In future work, we need to improve the performance of the watermarking algorithm regarding the high robustness, imperceptibility, security, and capacity of the information it can hold. We will also optimize the parameters and test using various modalities to get comprehensive results.

## Conflicts of Interest

The authors declare no conflict of interest.

## Author Contributions

Conceptualization, LDN and IDW; methodology, LDN, IDW, and NPW; software, LDN and NPW; validation, IDW; formal analysis, LDN, IDW, and NPW; investigation, LDN; resources, LDN and NPW; data curation, LDN; writing—original draft preparation, LDN and NPW; writing—review and editing, LDN and IDW; visualization, LDN; supervision, IDW; project administration, LDN; funding acquisition, LDN.

## Acknowledgments

This research is supported by Telkom University.

## References

- [1] H. Mani and S. Singh, “A Survey of Digital Watermarking Techniques and Performance Evaluation Metrics”, *Int. J. Eng. Trends Technol.*, Vol. 46, No. 2, pp. 128–132, 2017.
- [2] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, “Watermarking Techniques used in Medical Images: a Survey”, *J. Digit. Imaging*, Vol. 27, No. 6, pp. 714–729, 2014.
- [3] A. Meenpal, S. Majumder, and A. Balakrishnan, “Digital Watermarking Technique using Dual Tree Complex Wavelet Transform”, In: *Proc. of 2020 First International Conf. on Power, Control and Computing Technologies (ICPC2T)*, pp. 62–67, 2020.
- [4] N. Rathi and G. Holi, “Securing Medical Images by Watermarking Using DWT-DCT-SVD”, *Int. J. Comput. Trends Technol.*, Vol. 12, No. 2, pp. 67–74, 2014.
- [5] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, “An Efficient Medical Image Watermarking Scheme Based on FDCuT-DCT”, *Eng. Sci. Technol. an Int. J.*, Vol. 20, No. 4, pp. 1366–1379, 2017.
- [6] N. Mohananthini and G. Yamuna, “A Study of DWT-SVD Based Multiple Watermarking Scheme for Medical Images”, *Int. J. Netw. Secur.*, Vol. 17, No. 5, pp. 558–568, 2015.
- [7] S. D. Mashalkar and S. S. Shirgan, “Design of Watermarking Scheme in Medical Image Authentication using DWT and SVD Technique”, In: *Proc. of the International Conference on Computing Methodologies and Communication, ICCMC 2017*, pp. 955–960, 2018.
- [8] S. Ajili, M. A. Hajjaji, and A. Mtibaa, “Hybrid SVD-DWT Watermarking Technique using AES Algorithm for Medical Image Safe Transfer”, In: *Proc. of 16th International Conf. on Sciences and Techniques of Automatic Control and Computer Engineering, STA 2015*, No. December, pp. 69–74, 2016.
- [9] S. Gajula and V. Rajesh, “Medical Image Watermarking Scheme with DWT & SVD Transforms”, *Int. J. Pure Appl. Math.*, Vol. 117, No. 18, pp. 285–290, 2017.
- [10] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiyah, P. Yang, H. Huang, and G. Hou, “Secure and Robust Fragile Watermarking Scheme for Medical Images”, *IEEE Access*, Vol. 6, No. c, pp. 10269–10278, 2018.
- [11] I. Assini, A. Badri, K. S. A. Sahel, and A. Baghdad, “A Robust Hybrid Watermarking Technique for Securing Medical Image”, *International Journal of Intelligent Engineering and Systems*, Vol. 11, No. 3, pp. 169–176, 2018.
- [12] H. U. Seo, Q. Wei, S. G. Kwon, and K. I. Sohng, “Medical Image Watermarking Using Bit Threshold Map Based on just Noticeable Distortion in Discrete Cosine Transform”, *Technol. Heal. Care*, Vol. 25, No. S1, pp. S367–S375, 2017.

- [13] H. Ayad and M. Khalil, "QAM-DWT-SVD Based Watermarking Scheme for Medical Images", *Int. J. Interact. Multimed. Artif. Intell.*, Vol. 5, No. 3, p. 81, 2018.
- [14] M. Al-qdah, "Secure Watermarking Technique for Medical Images with Visual Evaluation", *Signal Image Process. An Int. J.*, Vol. 9, No. 1, pp. 01–09, 2018.
- [15] A. Mehto and N. Mehra, "Adaptive Lossless Medical Image Watermarking Algorithm Based on DCT & DWT", *Phys. Procedia*, Vol. 78, pp. 88–94, 2016.
- [16] S. Borra and R. Thanki, "Crypto-Watermarking Scheme for Tamper Detection of Medical Images", *Comput. Methods Biomech. Biomed. Eng. Imaging Vis.*, Vol. 00, No. 00, pp. 1–11, 2019.
- [17] U. Verma and N. Sharma, "Hybrid Mode of Medical Image Watermarking to Enhance Robustness and Imperceptibility", *Int. J. Innov. Technol. Explor. Eng.*, Vol. 9, No. 1, pp. 351–359, 2019.
- [18] N. Venkatram, L. S. S. Reddy, and P. V. V. Kishore, "Blind Medical Image Watermarking with LWT - SVD for Telemedicine Applications", *WSEAS Trans. Signal Process.*, Vol. 10, No. 1, pp. 288–300, 2014.
- [19] B. Madhu and G. Holi, "Medical Image Authentication by SWT and SVD", *Int. J. Recent Technol. Eng.*, Vol. 8, No. 3, pp. 953–958, 2019.
- [20] R. M. Thanki, V. J. Dwivedi, and K. R. Borisagar, "Multibiometric Watermarking Technique Using Fast Discrete Curvelet Transform (FDCuT) and Discrete Cosine Transform (DCT)", in *Multibiometric Watermarking with Compressive Sensing Theory*, pp. 137–160, 2018.
- [21] S. H. Soleymani, A. H. Taherinia, and A. H. Mohajerzadeh, "A Blind Robust Watermarking Method based on Arnold Cat Map and Amplified Pseudo-noise Strings with Weak Correlation", *Multimed. Tools Appl.*, Vol. 78, No. 14, pp. 19163–19179, 2019.
- [22] B. Furht, Ed., "Discrete Cosine Transform (DCT)", in *Encyclopedia of Multimedia*, Boston, MA: Springer US, pp. 203–205, 2006.
- [23] P. Geofisika, A. F. Sasti, and A. F. Sasti, "Komputasi Geofisika 1: Singular Value Decomposition untuk Matriks 5x5", 2018.
- [24] P. Kulkarni, S. Bhise, and S. Khot, "Review of Digital Watermarking Techniques", *Int. J. Comput. Appl.*, Vol. 109, No. 16, pp. 40–44, 2015.
- [25] D. B. Taha, T. Basheer Taha, and P. Ehkan, "Image Watermarking Algorithm Based on a Combination of Texture Mapping and Bit", *J. Theor. Appl. Inf. Technol.*, Vol. 97, No. 8, pp. 2206–2216, 2019.
- [26] F. N. Thakkar and V. K. Srivastava, "A Blind Medical Image Watermarking: DWT-SVD Based Robust and Secure Approach for Telemedicine Applications", *Multimed. Tools Appl.*, Vol. 76, No. 3, pp. 3669–3697, 2016.
- [27] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications", *Multimed. Tools Appl.*, Vol. 78, No. 3, pp. 3457–3470, 2019.