Received: December 18, 2019

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Image Watermarking Method Using Discrete Tchebichef Transform and Singular Value Decomposition Based on Chaos Embedding

Andik Setyono[1] **De Rosal Ignatius Moses Setiadi[1]***

[1]*Department of Informatics Engineering,*
Faculty of Computer Science, Dian Nuswantoro University, Semarang 50131, Indonesia
* Corresponding author's Email: moses@dsn.dinus.ac.id

Abstract: A good watermarking method should be robust against attacks but have good visual quality. This research proposes a combination of two transformations i.e. Tchebichef and singular value decomposition (SVD). Arnold's algorithm is also integrated to improve the security of the watermark and visual quality of the watermarked image. Arnold's transformation was carried out on the cover image with the aim to spread watermark. Furthermore, the cover image is divided into small blocks and transformed using Tchebichef. The lowest coefficient of each Tchebichef block is collected in a matrix for decomposition with SVD, then the watermark is embedded in the singular matrix. Based on the results of testing the proposed method can have excellent visual quality with PSNR values ranging from 45dB and SSIM averaging 0.998. The proposed method is also robust to various attacks such as filtering, noise addition, geometry, and signal processing.

Keywords: Chaos embedding, Copyright protection, Image watermarking, Singular value decomposition, Tchebichef.

1. Introduction

The development of internet technology today is extraordinary and applications for sharing files are increasingly sophisticated, making it easier to reproduce, manipulate and distribute multimedia data [1–3]. Some multimedia data certainly requires copyright protection, for example, data relating to medical, military, and having legal force. The watermarking technique is one of the methods used to protect copyright. Basically, watermarking is extended from the data hiding technique, then is used to protect cover images. There are two main objects in watermarking i.e. cover media and watermark as copyright, where the watermark embedded in the cover media has the duty to protect its cover media. Watermark must be robust embedded so that if there is manipulation or distortion on the cover media, the watermark is not damaged and can still be extracted for authentication. In addition to robustness, watermark imperceptibility must also be good for producing quality watermarking methods [4, 5].

Image is one of the most widely used cover objects in watermarking research. An image is an object that has two dimensions that can be felt by humans with a sense of sight so embedding a watermark on an image should not cause changes that can be detected by human vision. This is what is meant by imperceptibility in images watermarking. Currently, the development of research on image watermarking is very rapid. Many methods are proposed to improve the robustness and imperceptibility of image watermarking. But the trade-off between robustness and imperceptibility is always the opposite. Domain transformation methods such as DCT, DWT, and SVD are widely applied and proven to work well on image watermarking [4, 6–12], but each method still has advantages and disadvantages. The DCT method is a standard transformation used in JPEG compression, so by using this method, the results will generally be robust to compression attacks. Similarly, the DWT method used as a JPEG 2000 compression standard. Until now the use of JPEG compression is relatively more popular than JPEG 2000, the computational time

required is also relatively shorter when using the DCT method. While SVD has advantages in its resistance to geometric attacks such as rotational, flipping, and transpose attacks, besides that SVD is also robust to signal processing attacks [4, 13, 14]. This is what distinguishes SVD with DCT and DWT, so by combining it with the DCT, DWT or both methods, an increase in robustness and imperceptibility performance can be obtained [6, 7, 14]. One method that is relatively rarely used compared to the three methods above is Discrete Tchebichef Transform (DTT). DTT has many similarities with DCT, such as converging energy into the low-frequency region, orthogonal calculation bases, and how calculations can be done separately and symmetrically [15–17]. In several studies such as the studies [16] and [18], DCT and DTT methods have been compared, which results in robustness and imperceptibility performance which is very identical, even though the DTT method has faster computing time. In addition, the combination of DTT and DWT methods was also successfully applied in research [18], so that in this research a combination of DTT and SVD was conducted to test its performance, both in terms of imperceptibility, robustness and security.

On the security side, in various watermarking studies previously proposed encryption techniques on the watermark before being embedded. Watermarks can be encrypted by a variety of methods, from the simplest only with XOR operations, then to DES, RC4, or AES [19–21], and currently the most popular is the scramble technique based chaotic-map [22, 23]. Scramble technique is more suitable for encrypting multimedia data such as images because it is resistant to differential and statistical attacks, as well as minimizing the possibility of over computing due to the complexity of calculations [24, 25]. Another way to increase the security of a watermark is a non-sequential embedding technique. Sequential embedding is easy to guess and can be centered on one part of the cover image if the watermark image used is smaller than the capacity of the cover image. In a study conducted by Rachmawanto et al. [26], It is proposed a watermark embedding technique that is spread in whole images. With this technique, it is proven that there is an increase in the value of imperceptibility as measured by PSNR. In addition, indirectly the security of the watermark will be better maintained because it is not easily predictable by sequential extraction.

Based on the explanation above, the research proposed a combination of DTT and SVD methods based on chaotic embedding. Chaos operations are performed on the cover image, not on the watermark image, then the DTT transformation is based on small blocks, from each block the lowest coefficient is taken to be transformed again with SVD. Chaotic operations are used so that watermark embedding can be spread out and is relatively more secure and resistant to statistical and differential attacks. The initial DTT transformation aims to increase the resistance of the watermark against compression attacks and the addition of noise, while the SVD transformation is also used to increase resistance to geometry attacks. Furthermore, the watermark image is embedded in a singular section, so this method can obtain increased imperceptibility, robustness, and watermark security.

2. Preliminaries

2.1 Discrete tchebichef transform (DTT)

DTT and DCT are transformations derived from orthonormal tchebichef polynomials. DTT has many similarities with DCT, i.e. energy compactness, separability, orthogonality, and even symmetry [27]. But DTT has advantages in low complexity, reduce memory and faster computation than DCT [16, 28, 29]. The many similarities between DCT and DTT make DTT can be used as an alternative to DCT in its use in digital image processing. In various researches on image compression [27, 30, 31] and image watermarking[16, 18], it has been proven that DTT has a similar performance even slightly better compared to DCT. In some image watermarking researches such as [29, 32] it has also been proven that DTT has a very good performance. As with DCT, DTT operations are often performed by dividing the image into small blocks, which are generally 8×8 [16, 17, 27, 30], 4×4 [31] or 2×2 [33]. If there is a grayscale image (S) with a matrix size of 8 × 8, then the Tchebichef transformation (T) can be defined as Eq. (1).

$$T_{xy} = \begin{bmatrix} t_x(0)t_y(0) & t_x(0)t_y(1) & \dots & t_x(0)t_y(7) \\ t_x(1)t_y(0) & t_x(1)t_y(1) & \dots & t_x(1)t_y(7) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ t_x(6)t_y(0) & t_x(6)t_y(1) & \dots & t_x(6)t_y(7) \\ t_x(7)t_y(0) & t_x(7)t_y(1) & \dots & t_x(7)t_y(7) \end{bmatrix} \quad (1)$$

From Eq. (1), forward DTT has a definition written in Eq. (2).

$$T_{xy} = \sum_{x=0}^{7} \sum_{y=0}^{7} t_x(i) t_y(j) S(i,j) \quad (2)$$

From Eq. (2) there are orthonormal Tchebichef polynomials $t_x(i)$ and $t_y(j)$. Where degrees x and y can be defined in the discrete domain of $0,1,\dots 7$ which can be written in Eq. (3).

$$t_x(i) = (\alpha_1 i + \alpha_2)t_{u-1}(i) + \alpha_3 t_{x-2}(i) \quad (3)$$

Where $x \in [2,3,\dots,7]; x = 0$ is defined on Eq. (4) and $x = 1$ is defined in Eq. (5); Coefficient α_1 is defined in Eq. (6), α_2 is defined in Eq. (7), and α_3 is defined in Eq. (8).

$$t_0(i) = \frac{1}{\sqrt{8}} \quad (4)$$

$$t_1(i) = 2i + 1 - 8)\sqrt{\frac{3}{8(8^2-1)}} \quad (5)$$

$$\alpha_1 = \frac{2}{x}\sqrt{\frac{4x^2-1}{8^2-x^2}} \quad (6)$$

$$\alpha_2 = \frac{1-8}{x}\sqrt{\frac{4x^2-1}{8^2-x^2}} \quad (7)$$

$$\alpha_3 = \frac{x-1}{x}\sqrt{\frac{2x+1}{2x-3}}\sqrt{\frac{8^2-(8-1)^2}{8^2-x^2}} \quad (8)$$

Whereas to inverse DTT, formula (9) can be used.

$$S_{(i,j)} = \sum_{i=0}^{7}\sum_{j=0}^{7} T_{xy}t_x(i)t_y(j) \quad (9)$$

2.2 Singular value decomposition (SVD)

SVD is a transformation formula that functions to decompose an image matrix or pattern recognition into two orthogonal matrices and a singular matrix [7], [34]. In general, the SVD formula is written in Eq. (10).

$$M = USV^T \quad (9)$$

Where U, V are orthogonal matrices with dimensions $N \times N$; S is a singular matrix; T is transpose; M is an image matrix with dimensions $N \times N$, so it can be described as in Eq. (10).

$$\begin{aligned} &= [u_0, u_1, \dots, u_{N-1}] \times \\ &\begin{bmatrix} s_0 & & & \\ & s_1 & & \\ & & \ddots & \\ & & & s_{N-1} \end{bmatrix} \times [v_0, v_1, \dots, v_{N-1}]^T \\ &= \sum_{x=1}^{p} s_x u_x v_x^T \end{aligned} \quad (10)$$

Where x is the rank of M ($x \leq N$); u_x and v_x are right and left column vectors of the singular vector M, each of which satisfies Eq. (11).

$$U^T U = V^T V = I \quad (11)$$

Where I is the identity matrix.

In watermarking images, after the image matrix is decomposed using SVD, watermarks are generally embedded in a singular matrix. This matrix was chosen so that the watermark is resistant to various attacks, especially signal processing and geometry attacks [4, 13, 14]. If the watermark is embedded in the orthogonal matrix the imperceptibility can increase but is weak against attack or manipulation [34]. SVD also has several characteristics, namely, the singular value will be able to survive when there is a deviation, the main property, and image appearance are represented by a singular matrix, the light intensity in its value is determined by the singular matrix, while the geometry value is determined by the orthogonal matrix [35].

2.3 Arnold transform

One of image scrambling technique is Arnold transform. The scrambling process is done with Arnold's chaotic map. The results of the scrambling process can change the semantic characteristics of the image so as to increase the security effect [14, 23]. Although the semantic characteristics change, the histogram is the same as the original image. Arnold transform is also called an image encryption technique that is sensitive to initial values and resistant to differential attacks [36, 37]. In general, Arnold transform is mostly done on two-dimensional matrices that are defined as in Eq. (12).

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} mod\ M \quad (12)$$

Where p and q are positive integers, i and j are the designated pixel coordinates, M is the dimension of height or width of the matrix, where the width and height of the matrix are the same. Eq. (12) will be carried out in an iteration process called the Arnold

period, wherein the scrambling process can be done based on certain Arnold periods that can be determined[38]. Whereas to inverse Arnold transform can use the notation (13). In the inverse Arnold transforms, process must use the same number of iterations.

$$\begin{bmatrix} i \\ j \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}^{-1} \begin{bmatrix} i' \\ j' \end{bmatrix} mod\ M \qquad (13)$$

In general, Arnold transform is carried out on a watermark image, before it is embedded in a Cover image. But in this research Arnold transform was carried out on the cover image with the aim of watermark embedding techniques that spread throughout the entire image randomly. This is done with the aim of replacing the pseudo-random generator function in the spread spectrum technique to increase the imperceptibility and security of the watermark[26].

3. Proposed method

3.1 Watermark embedding procedure

In the process of embedding a watermark, there are three things that must be inputted, namely the cover image, the watermark image or copyright and the key to the scrambling process using Arnold transform. While the output produced is a watermarked image, the details are explained in the following steps:

Step 1: Read the key (k) and original cover image (C), then scramble the original cover image based on the key. Where the key will be processed to determine the value of p and q in accordance with Eq. (12) and determine the Arnold period. The result in this step is the scrambled cover image (S).

Step 2: Break the S matrix in small 8x8 non-overlapping dimensions.

Step 3: Transform the Tchebichef forward on each block using formula (2).

Step 4: Take the coefficient (0,0) on each block. This coefficient is chosen to get robustness in the watermark. For the record, the coefficient (0,0) has an identical character with a DC coefficient on the DCT.

Step 5: Collect coefficients (0,0), become a matrix (Z), then decompose the matrix using SVD transformations. Then the U_z, V_z and S_z matrices will be generated.

Step 6: On the other hand, read the watermark image (W), then do an SVD transformation to decompose the watermark image. Then the resulting matrix U_w, V_w dan S_w.

Step 7: Embed S_w to S_z by multiplying the value of S_w with a certain weight (α), then adding it to S_z so that it produces S_m. Where this weight is sensitive to the level of imperceptibility and robustness

Step 8: Get the modified Z matrix (Z') with the inverse SVD on the Z matrix whose singular value has been replaced with S_m.

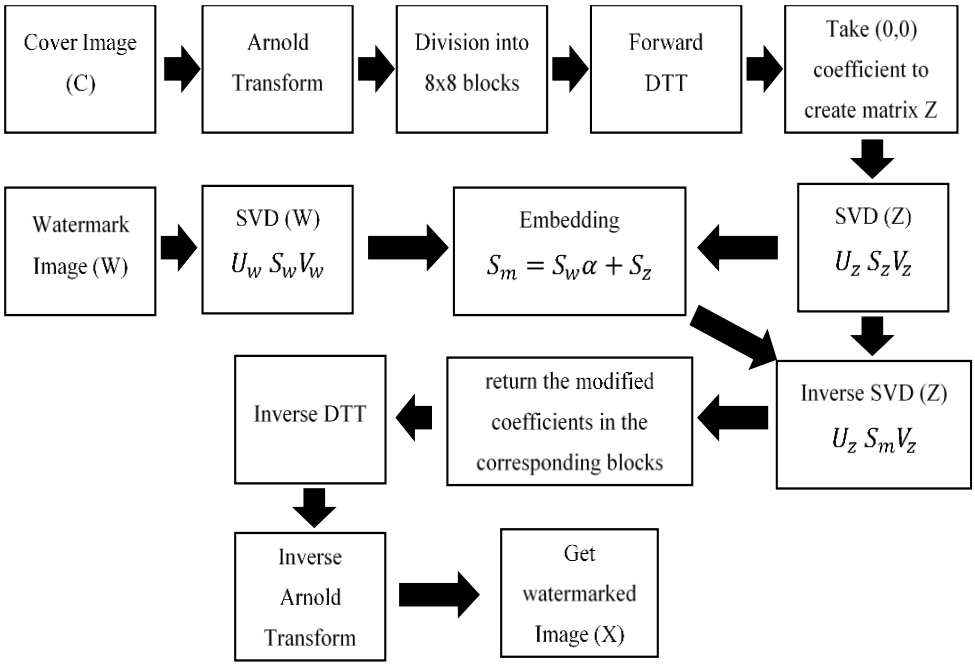

Figure. 1 Watermark embedding procedure

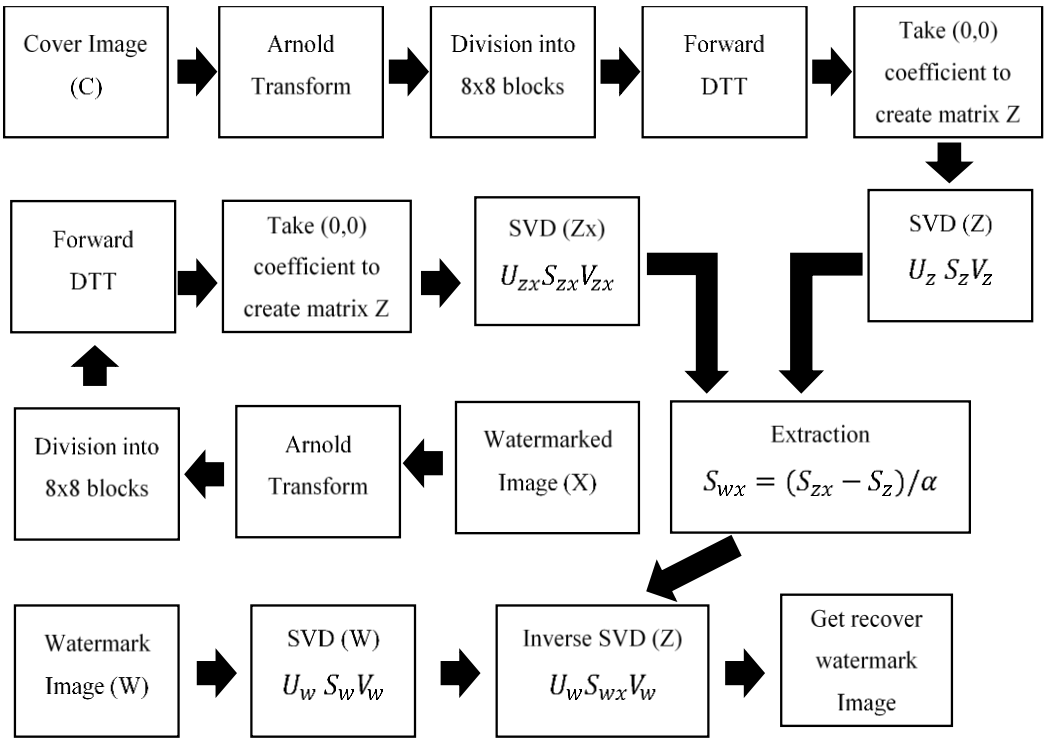

Figure. 2 Watermark extraction procedure

Step 9: Take each cell from the Z' matrix, then place it back on the coefficient (0,0) of each block.

Step 10: Perform the Tchebichef inverse transformation to get the watermarked image (X).

Step 11: descramble the X image with Eq. (13) based on k.

To understand more clearly can see Fig. 1.

3.2 Watermark extraction procedure

Whereas the watermark extraction in detail is explained in the following steps:

Step 1: Read the watermarked image (X), the original cover image (C), and the key (k), then scramble the matrix X and C based on the key. The results in this step are scrambled cover image (S) and scrambled watermarked image (Sx).

Step 2: Break the S matrix in small blocks of 8x8 non-overlapping dimensions, also do the Sx matrix.

Step 3: Transform the Tchebichef forward for each block using Eq. (2).

Step 4: Take the coefficients (0,0) for each block, then collect the coefficients on the Z matrix for S and Zx matrix for Sx.

Step 5: Perform matrix decomposition using SVD transforms. Then the U_z, V_z and S_z matrices for the Z matrix and U_{zx}, V_{zx} and S_{zx} for the Zx matrix will be generated.

Step 6: Extract the watermark by subtracting the value of S_{zx} with S_z, then dividing it by the same weight (α) value as the embed process, so that it produces S_{wx}.

Step 7: Read the watermark image (W), then do an SVD transformation, then a matrix is produced U_w, V_w and S_w matrices.

Step 8: Perform an inverse SVD with the U_w, V_w and S_{wx} matrices to get the recover watermark image.

To understand more clearly can see Fig. 2.

4. Results and Discussion

In this section, the method described in the previous section is implemented. The results of the implementation of the proposed method are measured with standard measuring instruments such as MSE, PSNR, and SSIM, to determine the visual quality of the watermarked image. Meanwhile, to know the robustness performance is measured by NC as a measurement tool. In order to be compared with the previous method, a standardized test image is used, the image is presented in Fig. 3. This image is used as a cover image, where the image has 512x512 dimension specifications with a depth of 8 bits. In Fig. 3 also presented a binary image as a 64x64 watermark.

Next, watermark embed on the cover image is done, so that the resulting watermarked image is presented in Fig. 4.

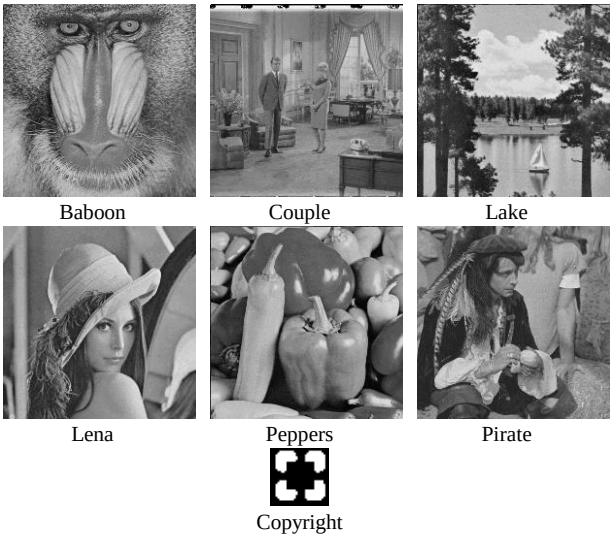

Figure. 3 Cover test image and copyright logo

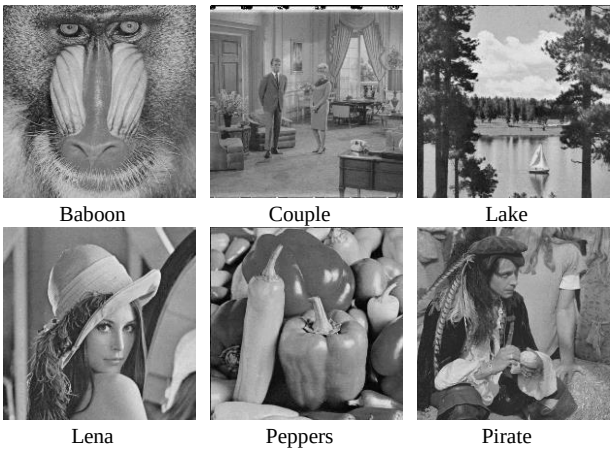

Figure. 4 Watermarked image results

It can be seen that the results obtained by the naked eye have no difference. This is called imperceptibility, where embedded watermarks cannot be perceived by the human sense of sight. Other terms also say that watermarks are invisible. But visual assessment is certainly not enough, standard measurements with numerical results are needed to determine the quality of visual watermarked images. Where the visual quality is measured using MSE generated from the difference between the original cover image and the watermarked image that can be calculated by the formula (14). It also measured the value of PSNR generated from the MSE logarithm value, PSNR can be calculated by the formula (15). The last measurement is to use SSIM, which is the difference between the calculation of intensity, contrast and the structure of the difference between the original cover image with a watermarked image, which can be measured by formula (16). Whereas the results of the measurement of visual watermarked images are presented in Table 1.

Table 1. Visual measurement of watermarked image results based on MSE, PSNR, and SSIM

Image	MSE	PSNR	SSIM
Baboon	1.7920	45.5974	0.9991
Couple	1.8444	45.4723	0.9980
Lake	1.9512	45.2278	0.9986
Lena	1.9541	45.2213	0.9985
Peppers	1.8467	45.4669	0.9975
Pirate	1.9053	45.3312	0.9987
Average	1.8823	45.3862	0.9984

$$MSE = \frac{1}{w \times h} \sum_{m=1}^{w} \sum_{n=1}^{h} \| X(m,n) - C(m,n) \|^2 \quad (14)$$

$$PSNR_{(dB)} = 10 \times Log\, 10 \left(\frac{255^2}{\sqrt{MSE}} \right) \quad (15)$$

$$SSIM\,(X,C) = \frac{(2\mu_x\mu_C + v_1)(2\sigma_{xC} + v_2)}{(\mu_x^2 + \mu_C^2 + v_1)(\sigma_x^2 + \sigma_C^2 + v_2)} \quad (16)$$

X is a watermarked image; C is an original cover image; w and h are the image dimension; m, n are pixel locations; μ_x is mean of the X; μ_C is mean of the C; σ_{xC} is the covariance X against C; σ_x^2 is a variant of X; σ_C^2 is a variant of C; $v_1 = (l_1 D)^2$ and $v_2 = (l_2 D)^2$; D is a dynamic range $(2^{bits} - 1)$ with the default value $l_1 = 0.01$ dan $l_2 = 0.03$.

The next test is the robustness of the watermark. A watermarking method will not work well if only one aspect is fulfilled. The imperceptibility, robustness and security aspects must be fully fulfilled. Especially in the aspect of robustness, it becomes very important because this aspect serves to provide copyright protection. To test robustness in this study, several manipulations or attacks are described in Table 2. Manipulation is done on watermarked images, samples of the results of manipulations of watermarked images are presented in Fig. 5.

After manipulating the watermarked image, a watermark extraction test is performed. This test aims to determine whether the embedded watermark can still survive the given manipulation. The results of watermark extraction can be seen in Table 3.

The results presented in Table 3 show that most of the watermark can still be extracted, the following pattern and shape can still be recognized. The proposed method, which is a combination of discrete

Table 2. Attack description for robustness test

Index of Attack	Description
0	Without attack
1	2×2 Median filtering
2	Rescaling (512 → 256 → 512)
3	Gamma correction (0.2)
4	270^0 rotation
5	Histogram equalization
6	JPEG Compression with Q=75
7	Salt and pepper 0.05
8	Cropping (20480 pixels)
9	Gaussian noise (0.02)
10	Blur Filter
11	Flip Columns
12	Flip Rows

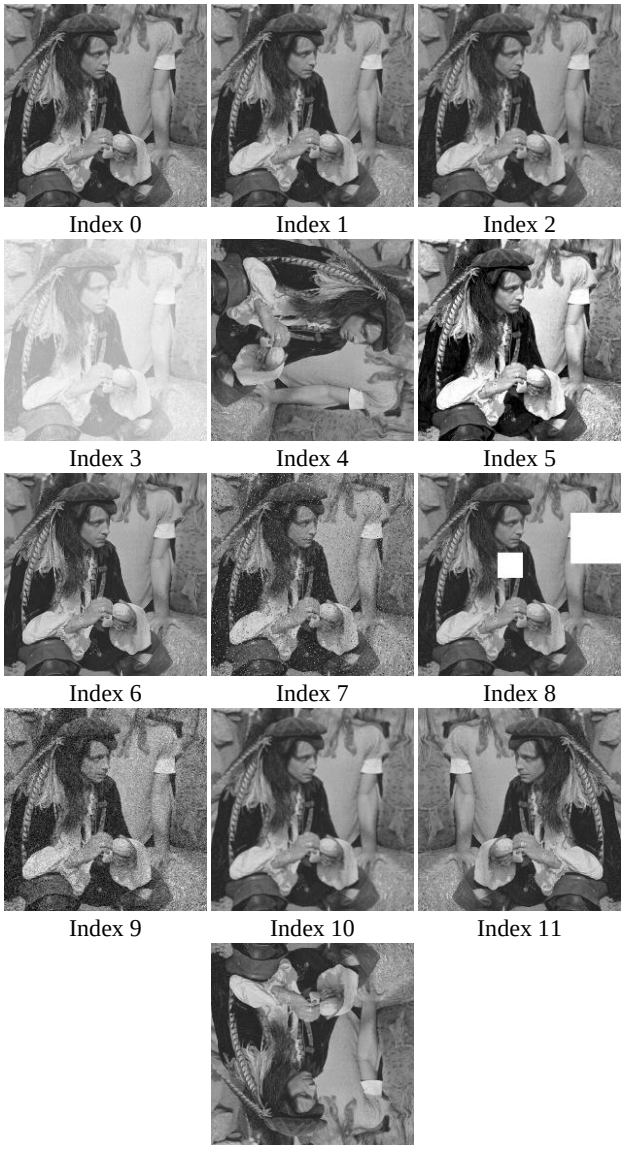

Figure. 5 Display of the results of attacks that are applied from one of the cover images

Table 3. Extracted watermark results

Index	Baboon	Couple	Lake	Lena	Peppers	Pirate
0						
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

tchebichef transform (DTT) and singular value decomposition (SVD), is a non-blind method that is robust but has a high imperceptibility quality. However, the contribution of the method to this research can be measured more clearly if compared with previous research. One of them is done by Ali et al. [39], in his research a combination of DCT and SVD methods is proposed for embedding watermarking, this combination of methods can produce high robustness and high enough imperceptibility. In his research also used Arnold transform which is imposed on the watermark image to improve security. It should be noted that the proposed method has a similarity, which used a combination of two transformations for the embedding process and Arnold transform. The difference between the DCT method is replaced with the DTT method, and Arnold transform implementation is not done on the watermark image but on the cover image.

Other research conducted by Tuncer and Kaya [22] uses the same dataset with the two-level wavelet

Table 4. Description of the compared method and proposed method

Property	Ali et al [39]	Tuncer and Kaya [22]	Proposed
Cover Image	512×512	512×512	512×512
Watermark	32×32	64×64	64×64
Domain	Transform	Transform	Transform
Visual Logo	Yes	Yes	Yes
Payload	0.0156	0.0156	0.0156

Table 5. Comparison PSNR values from several methods

Image	Ali et al [39]	Tuncer and Kaya [22]	Proposed
Baboon	40.03	62.94	45.60
Couple	42.01	67.07	45.47
Lake	40.00	64.38	45.23
Lena	44.02	66.20	45.22
Peppers	43.02	66.12	45.47
Pirate	45.02	64.24	45.33
Average	42.35	65.16	45.39

transformation method based on blocks combined with encryption methods to increase the security of the watermark, resulting in very high imperceptibility and security performance but robustness is still lacking. Then the proposed method can be used as an alternative method that can be chosen, as a comparison description of the proposed method with the previous method can be seen in Table 4.

It can be seen that based on the properties presented in Table 4, the two previous methods are balanced for comparison. Comparison of PSNR values presented can be seen in Table 5.

Based on Table 5, it appears that the proposed method has a better PSNR than the Ali et al [39], the imperceptibility value can be better because of the use of the Arnold transformation on the cover image, it aims to embed a spread watermark so as to increase imperceptibility and security. But the PSNR not better than the method proposed by Tuncer and Kaya [22]. As discussed earlier, in addition to imperceptibility watermark robustness is also required, the robustness can be measured by normalized correlation (NC), which can be calculated by the formula (17). The NC calculation results and comparison with the previous method are presented in Table 6 for extraction without manipulation and Table 7 for extraction by manipulation.

$$NC = \sum_{m=1}^{w} \sum_{n=1}^{h} \frac{w_{mn} \overline{\oplus} e_{mn}}{w \times h} \quad (17)$$

Table 6. Comparison of NC values without attack from several methods

Image	Ali et al [39]	Tuncer and Kaya [22]	Proposed
Baboon	1.0000	1.0000	1.0000
Couple	1.0000	1.0000	1.0000
Lake	1.0000	1.0000	1.0000
Lena	1.0000	1.0000	1.0000
Peppers	1.0000	1.0000	1.0000
Pirate	0.9922	1.0000	1.0000
Average	0.9987	1.0000	1.0000

Table 7. Comparison of NC values with attack from several methods

Index	Ali et al [39]	Tuncer and Kaya [22]	Proposed
0	0.9987	**1.0000**	**1.0000**
1	0.9076	0.5200	**0.9895**
2	0.9134	0.4600	**0.9688**
3	**0.9973**	0.6600	0.7136
4	**0.9988**	0.5100	0.9382
5	**0.9982**	0.6200	0.7639
6	0.9574	0.4600	**0.9981**
7	0.8104	0.8400	**0.9492**
8	-	-	0.7218
9	-	-	0.9459
10	-	-	0.9332
11	**0.9988**	-	0.7965
12	**0.9988**	0.5300	0.7707

Where w is original watermark image; e is extracted watermark image

Based on the results presented in Table 6 and Table 7, it appears that the proposed method can perfectly extract all watermarked images that have not been manipulated. Whereas after being manipulated the proposed method is superior to attacks that have indexes 1, 2, 6 and 7, while the method of Ali et al [39] is superior to attacks that have indexes 3,4,5, 11, and 12, for the Tuncer and Kaya [22] does not have the advantage in any attack but can extract watermarks perfectly on watermarked images that are not manipulated. In short, although the proposed method cannot have imperceptibility as well as the method in [22], the proposed method can provide an increase in PSNR value of about 3 dB when compared to the method in [39]. The robustness aspect is also maintained even though it has different advantages in the type of manipulation that is applied.

5. Conclusion

This research successfully combined two transformations i.e. DTT and SVD. The use of DTT was chosen as an alternative to DCT. DTT is known to have faster performance and computation compared to DCT but has identical advantages with

DCT. Whereas SVD has an advantage in a good decomposition process and is resistant to geometry and signal processing. These two transformations are combined with scramble embedding techniques using the Arnold transformation, which is used to increase the security of the watermark and visual output. Based on the results of tests that have been carried out the proposed watermarking method is proven to have good performance, where the visual quality is very good with PSNR values ranging from 45dB and SSIM averaging 0.998. The robustness test also shows that although the visual results are very good, it can be more integrated into some attack models compared to the previous method.

In the future this research can be developed by combining with several other transformation methods with more decomposition levels, it can also be combined with artificial intelligence methods for automating embedment parameters and optimizing results.

Acknowledgment

The authors would like to express very special thanks to the Ministry of Research, Technology and Higher Education Republic of Indonesia for providing financial support of this research project with letter number: 026/L6/AK/SP2H.1/PENELITIAN/2019.

References

[1] T. Venugopal, V. Siva, and K. Reddy, "Image Watermarking Using Two Level Encryption Method Based on Chaotic Logistic Mapping and Rivest Shamir Adleman Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 11, No. 6, pp. 271-281, 2018.

[2] N. N. Mood and V. Subbareddy Konkula, "A Novel Image Watermarking Scheme Based on Wavelet Transform and Genetic Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 11, No. 3, pp. 251-260, 2018.

[3] D. R. I. M. Setiadi, "Improved payload capacity in LSB Image Steganography uses dilated hybrid edge detection", *J. King Saud Univ. - Comput. Inf. Sci.*, 2019.

[4] T. K. Araghi, A. A. Manaf, and S. K. Araghi, "A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition", *Expert Syst. Appl.*, Vol. 112, pp. 208–228, Dec. 2018.

[5] S. Wang, X. Meng, Y. Yin, Y. Wang, X. Yang, X. Zhang, X. Peng, W. He, G. Dong, and H. Chen, "Optical image watermarking based on singular value decomposition ghost imaging and lifting wavelet transform", *Opt. Lasers Eng.*, Vol. 114, pp. 76–82, 2019.

[6] H.-T. Hu and L.-Y. Hsu, "Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression", *Comput. Electr. Eng.*, Vol. 41, pp. 52–63, 2015.

[7] X. Wu and W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD", *Appl. Soft Comput.*, Vol. 13, No. 2, pp. 1170–1182, 2013.

[8] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm", *Expert Syst. Appl.*, Vol. 41, No. 17, pp. 7858–7867, 2014.

[9] Poonam and S. M. Arora, "A DWT-SVD based Robust Digital Watermarking for Digital Images", *Procedia Comput. Sci.*, Vol. 132, pp. 1441–1448, 2018.

[10] O. Jane, E. Elbaşi, and H. G. İlk, "Hybrid Non-Blind Watermarking Based on DWT and SVD", *J. Appl. Res. Technol.*, Vol. 12, No. 4, pp. 750–761, 2014.

[11] L.-Y. Hsu and H.-T. Hu, "Robust blind image watermarking using crisscross inter-block prediction in the DCT domain", *J. Vis. Commun. Image Represent.*, Vol. 46, pp. 33–47, 2017.

[12] I. Assini, A. Badri, K. Safi, 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.

[13] S. Fazli and M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks", *Optik (Stuttg).*, Vol. 127, No. 2, pp. 964–972, 2016.

[14] M. Ali, C. W. Ahn, and M. Pant, "A robust image watermarking technique using SVD and differential evolution in DCT domain", *Optik (Stuttg).*, Vol. 125, No. 1, pp. 428–434, 2014.

[15] F. Ernawan, M. N. Kabir, M. Fadli, and Z. Mustaffa, "Block-based Tchebichef image watermarking scheme using psychovisual threshold", In: *Proc. of the 2016 2nd International Conference on Science and Technology-Computer (ICST)*, pp. 6–10, 2016.

[16] D. R. I. M. Setiadi, T. Sutojo, E. H. Rachmawanto, and C. A. Sari, "Fast and efficient image watermarking algorithm using discrete tchebichef transform", In: *Proc. of 2017 5th International Conference on Cyber and IT Service Management (CITSM)*, pp. 1–5, 2017.

[17] R. Noor, A. Khan, A. Sarfaraz, Z. Mehmood,

and A. M. Cheema, "Highly robust hybrid image watermarking approach using Tchebichef transform with secured PCA and CAT encryption", *Soft Comput.*, pp. 1–9, 2019.

[18] A. Setyono and D. R. I. M. Setiadi, "Image Watermarking using Discrete Wavelet-Tchebichef Transform", *Indones. J. Electr. Eng. Comput. Sci.*, Vol. 16, No. 3, pp. 1416–1423, 2019.

[19] S. Ajili, M. A. Hajjaji, and A. Mtibaa, "Hybrid SVD-DWT watermarking technique using AES algorithm for medical image safe transfer", In: *Proc. of 2015 16th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, pp. 69–74, 2015.

[20] M. P. Shareef, T. V. Divya, N. Abraham, T. Babu, and K. V. Reshma, "Encryption-enhanced reversible watermarking for medical images via prediction and RC4 encryption", In: *Proc. of 2014 International Conference on Communication and Signal Processing*, pp. 1509–1513, 2014.

[21] A. Fierro-Radilla, M. Nakano-Miyatake, M. Cedillo-Hernandez, L. Cleofas-Sanchez, and H. Perez-Meana, "A Robust Image Zero-watermarking using Convolutional Neural Networks", In: *Proc. of 2019 7th International Workshop on Biometrics and Forensics (IWBF)*, pp. 1–5, 2019.

[22] T. Tuncer and M. Kaya, "A novel image watermarking method based on center symmetric local binary pattern with minimum distortion", *Optik (Stuttg).*, Vol. 185, pp. 972–984, 2019.

[23] M. Khalili, "DCT-Arnold chaotic based watermarking using JPEG-YCbCr", *Optik (Stuttg).*, Vol. 126, No. 23, pp. 4367–4371, 2015.

[24] S. Kandar, D. Chaudhuri, A. Bhattacharjee, and B. C. Dhara, "Image encryption using sequence generated by cyclic group", *J. Inf. Secur. Appl.*, Vol. 44, pp. 117–129, 2019.

[25] A. Broumandnia, "Designing digital image encryption using 2D and 3D reversible modular chaotic maps", *J. Inf. Secur. Appl.*, Vol. 47, pp. 188–198, 2019.

[26] E. H. Rachmawanto, D. R. I. M. Setiadi, C. A. Sari, and N. Rijati, "Imperceptible and secure image watermarking using DCT and random spread technique", *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, Vol. 17, No. 4, 2019.

[27] R. K. Senapati, U. C. Pati, and K. K. Mahapatra, "Image Compression Using Discrete Tchebichef Transform Algorithm", In: *Proc. fo International Conference on Advances in Communication, Network, and Computing*, 2010.

[28] P. A. M. Oliveira, R. J. Cintra, F. M. Bayer, S. Kulasekera, and A. Madanayake, "Low-Complexity Image and Video Coding Based on an Approximate Discrete Tchebichef Transform", *IEEE Trans. Circuits Syst. Video Technol.*, Vol. 27, No. 5, pp. 1066–1076, 2017.

[29] F. Ernawan, "Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection", *Int. J. Electr. Comput. Eng.*, Vol. 9, No. 3, pp. 1850–1860, 2019.

[30] K. K. Mahapatra, U. C. Pati, and R. K. Senapati, "Reduced memory, low complexity embedded image compression algorithm using hierarchical listless discrete Tchebichef transform", *IET Image Process.*, Vol. 8, No. 4, pp. 213–238, 2014.

[31] H. I. Saleh, "A Fast Block-Pruned 4x4 DTT Algorithm for Image Compression", *Int. J. Comput. Theory Eng.*, pp. 258–261, 2009.

[32] C. Deng, X. Gao, X. Li, and D. Tao, "A local Tchebichef moments-based robust image watermarking", *Signal Processing*, Vol. 89, No. 8, pp. 1531–1539, 2009.

[33] F. Ernawan, E. Noersasongko, and N. A. Abu, "An efficient 2×2 Tchebichef moments for mobile image compression", In: *Proc. of 2011 International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS)*, pp. 1–5, 2011.

[34] C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Robust and imperceptible image watermarking by DC coefficients using singular value decomposition", In: *Proc. of International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2017.

[35] V. Santhi and A. Thangavelu, "DC Coefficients Based Watermarking Technique for color Images Using Singular Value Decomposition", *Int. J. Comput. Electr. Eng.*, Vol. 3, No. 1, pp. 8–16, 2011.

[36] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption", *Signal Processing*, Vol. 147, pp. 133–145, 2018.

[37] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box", *Chaos, Solitons & Fractals*, Vol. 95, pp. 92–101, 2017.

[38] E. J. Kusuma, C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "A Combination of

Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography", *J. ICT Res. Appl.*, Vol. 12, No. 2, p. 103, 2018.

[39] M. Ali, C. W. Ahn, M. Pant, and P. Siarry, "An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony", *Inf. Sci. (Ny).*, 2015.