

---

## Digital Image Copyright Protection with Spatial Domain Public Image Watermarking Scheme

Mawaddah Harahap<sup>1)\*</sup>, Johannes Rianto Malau<sup>2)</sup>, Tentus Natoka S<sup>3)</sup>, Davin Winata<sup>4)</sup>, David Hadyanto<sup>5)</sup>

<sup>1)2)3)4)5)</sup>Universitas Prima Indonesia, Medan, Indonesia.

<sup>1)</sup>[mawaddah@unprimdn.ac.id](mailto:mawaddah@unprimdn.ac.id), <sup>2)</sup>[johannesrianto709@gmail.com](mailto:johannesrianto709@gmail.com), <sup>3)</sup>[natokatentus@gmail.com](mailto:natokatentus@gmail.com),

<sup>4)</sup>[davinwinata58@gmail.com](mailto:davinwinata58@gmail.com), <sup>5)</sup>[david.hadyanto11@gmail.com](mailto:david.hadyanto11@gmail.com)

---

### ABSTRACT

The resulting digital image certainly has the copyright attached to the image. There needs to be protection of digital image works because the form of storage of digital imagery works that are vulnerable to piracy, claims of unauthorized authorities, illegal duplication, or unauthorized modification. The Spatial Domain Public Image Watermarking method is used to protect digital imagery using applications designed to facilitate the watermarking process on several different digital images as well as with different image formats. The reason for using this method is because it has low complexity. In this study, it consisted of three processes carried out, namely the process of making watermarking, the process of checking watermarking and comparison of input imagery and image results. In the process of making watermarking do image input as a watermarking media, input inserted imagery in the form of binary images / text, key inputs and watermark results. In process of checking watermarking performs image input that becomes watermark media, watermark results input, key input, and checking results. The process of creating watermarking takes a relatively short time while the process of extracting watermarking processing time depends on the size of the image file. From some image testing conducted using imagery with three formats, namely: JPG with an average time accuracy of 9:5.310(42.15%), .GIFs with an average time of 8:27.207(21.63%), and. BMP has an average time accuracy of 5:2.989(36.22%). Thus, the determination of the image format used is adjusted to the original image, so that it can perform time efficiency.

**Keywords:** Copyright Protection, Digital Image, Spatial Domain Public, Watermarking Method, Watermarking Scheme.

---

### INTRODUCTION

The increasing number of works of art in the form of images and images produced by artists in digital form using image processing applications that are poured into digital media (Alfred T, Ronal F. S, Setia B, 2016). Digital images are objects that are very easy to change or manipulate, copied irresponsibly. It is difficult to prove that the image has been altered by the current media, and it is also difficult to prove its ownership (Suheryadi, 2017). In today's digital era, the internet has become a daily necessity, which makes it easy for users to carry out file transmission activities, thus requiring protection from irresponsible actors (Ondi & Dedy, 2021). This ease of accessing digital data makes someone who is not entitled or irresponsible to abuse the copyright of others (Febriani, 2016). One of the efforts to combat copyright infringement can be done with steganography. Steganography (steganography) is the science and art of hiding a secret message (hiding message) so that the existence of the message is not detected by the human senses (Imami et al., 2019). Watermarking is one of the sciences of hiding data with the aim of securing images, one of which is copyright protection (Susanto et al., 2017). The watermarking method is used to protect medical images from unauthorized misuse using the Singular Value Decomposition (SVD) and Particle Swarm Optimization (PSO) methods. Between medical images and watermarked medical images (Gangdhar et al., 2018).

Many photo agencies expose their collections on websites with the view of selling image access. By creating thumbnail web pages it is possible to purchase high resolution images. However, this flexibility to utilize digital images facilitates information piracy. Cryptographic techniques can solve the problem of unauthorized access to information. But it cannot prevent unauthorized users from replicating the decrypted content illegally (Surekha & Swamy, 2016). Efforts to minimize crimes committed in copyright infringement and document falsification. Important document protection can be done by applying the Watermarking Content Based Image Retrieval (CBIR) technique (Wasilah et al., 2016). Watermarking technique is one solution to avoid illegal copying. Currently, many watermarking

\* Corresponding author



This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

schemes have been proposed to overcome this problem (Herawati, 2019). The development of internet technology provides convenience in daily activities in obtaining digital data. Someone easily has the right to claim digital data so that it can cause problems in the copyright of a data (Kurniawan et al., 2018). Digital images that are private and confidential are highly susceptible to eavesdropping by other parties, especially if the images are distributed over the internet. The act of wiretapping and misuse of confidential images can of course harm the owner of the image (Zebua & Ndruru, 2017). The resulting digital image of course has a copyright attached to the image. There is a need for protection of digital image works because the form of storing digital image works is vulnerable to piracy, claims by unauthorized parties, illegal duplication, or unauthorized modification.

## METHOD

### Type of Research

This research uses this type of quantitative research, by conducting experiments on testing multiple sample datasets as a trial in calculating the accuracy of the algorithms used as proposed solutions in performing image protection as legitimate copyright. With multiple image inputs that are BMP, GIF, and JPG as well as text files with .txt extensions, which are inputted into applications designed to help facilitate image testing. The Spatial Domain Public Image Watermarking method is used to protect digital imagery using applications designed to facilitate the watermarking process on several different digital images as well as with different image formats. The reason for using this method is because it has low complexity.

### Time and Place of Research

This study took approximately 1 year and has been implemented from January 2021.

### Working Procedures

The application to be designed will be depicted and modeled using a use case:

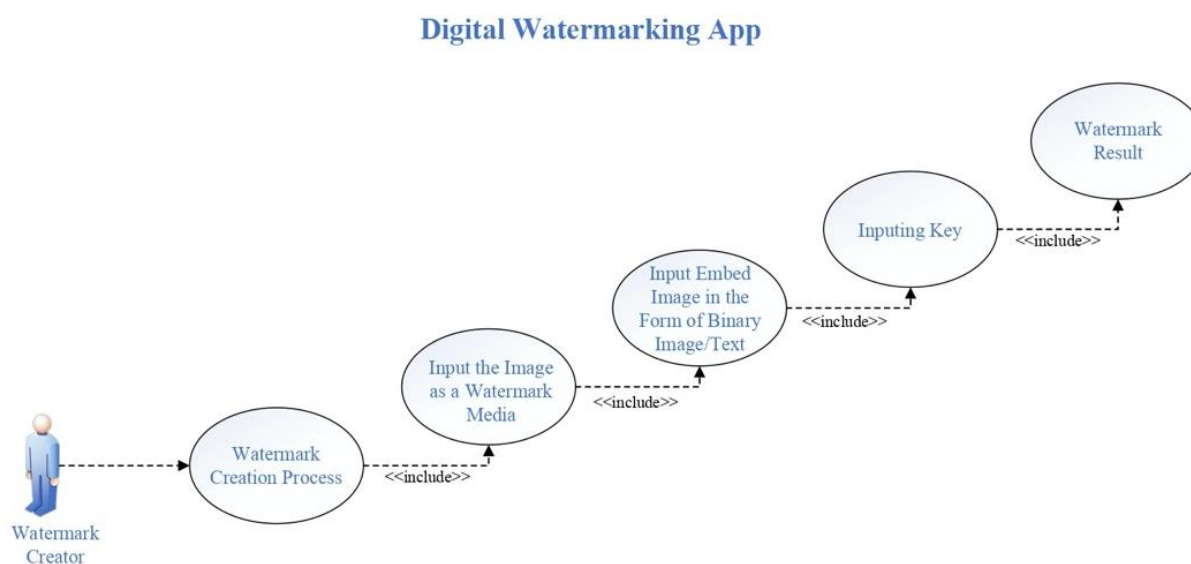


Fig. 1 Use Case Watermark Maker Diagram

\* Corresponding author



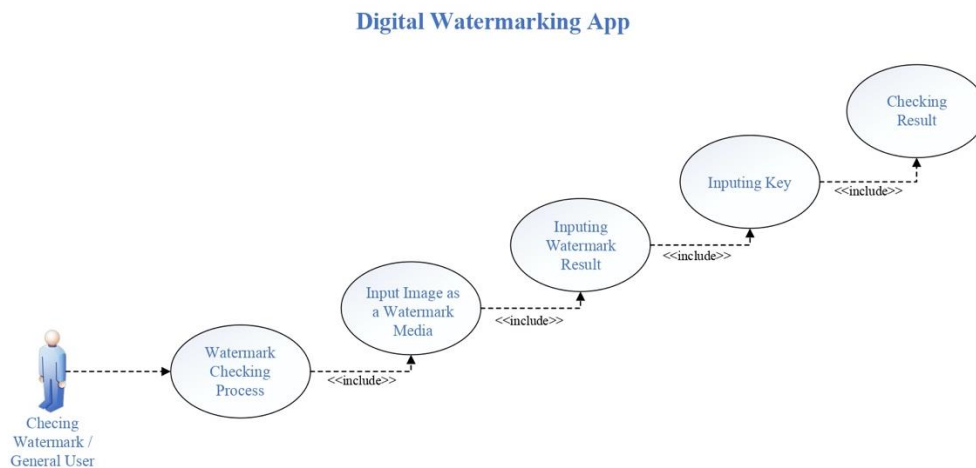


Fig. 2 Use Case Watermark Checking Diagram

As seen in figure 1, the entities of the application only number two pieces: watermarking maker, watermarking extractor and attacker. Meanwhile, the process contained in the software there are five pieces, namely doing the process of making watermarking, doing the process of checking watermarking, opening image files, storing image files, and displaying the results of the calculation process.

The working procedure of the Spatial Domain Public Image Watermarking scheme application is outlined in an activity diagram as follows:

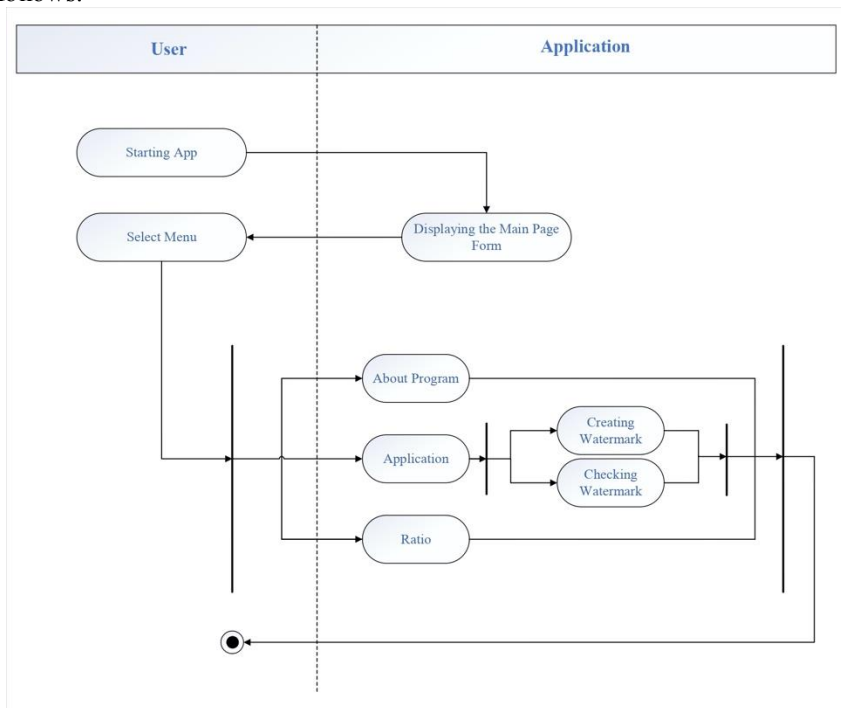


Fig. 3 User Activity Diagram

When the user runs the application, the Spatial Domain Public Image Watermarking schema application will display the main page of the application for the user. On the main page, the application will display several menus for the user. If the user selects a menu about the program, the application will display a form about the program. Meanwhile, if the user chooses the application menu, then the application will display two additional options,

\* Corresponding author



namely the watermarking creation menu and the watermarking check menu. If the user chooses the watermarking menu, the application will display a watermarking creation form. Meanwhile, if the user chooses the watermarking check menu, the application will display a watermarking checking form.

The design of the activity diagram depicting the process of creating watermarking on the software can be seen in figure 4. Here:

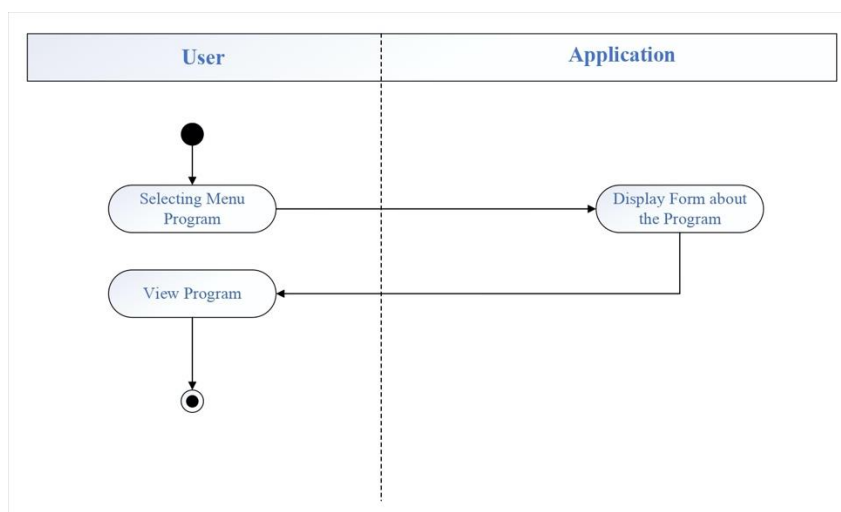


Fig. 4 Activity Diagram Of The Program

When the user selects the supporting theory menu, the application will display a supporting theory form that contains a brief discussion of the Spatial Domain Public Image Watermarking scheme and also the procedure of creating and extracting watermarks.

### System Analysis

The entities of the application only number three pieces namely watermarking makers, watermarking extractors and attackers. Meanwhile, the process contained in the software there are five pieces, namely doing the process of making watermarking, doing the process of checking watermarking, opening image files, storing image files, and displaying the results of the calculation process. Watermarking in its application to digital data can be classified into two parts, one of which is spatial domain. The reason for the selection of this method is that it has such low computational complexity that it is suitable for practical application.

### RESULT

The following is a look at the application at the watermarking extracting process stage.

1. Watermarking creation after process (Binary Image Insertion).

\* Corresponding author



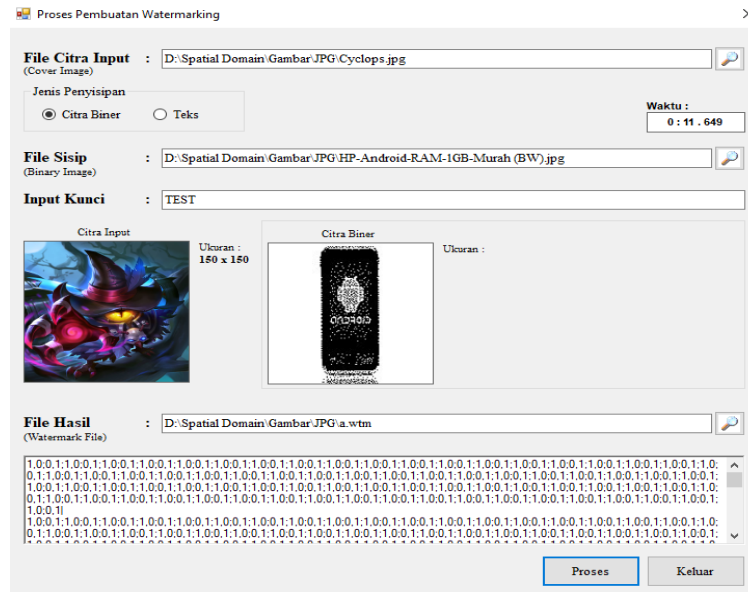


Fig. 5 Creation of Watermarking After Process (Insertion of Binary Images)

2. Watermarking creation after process (Text Insertion).

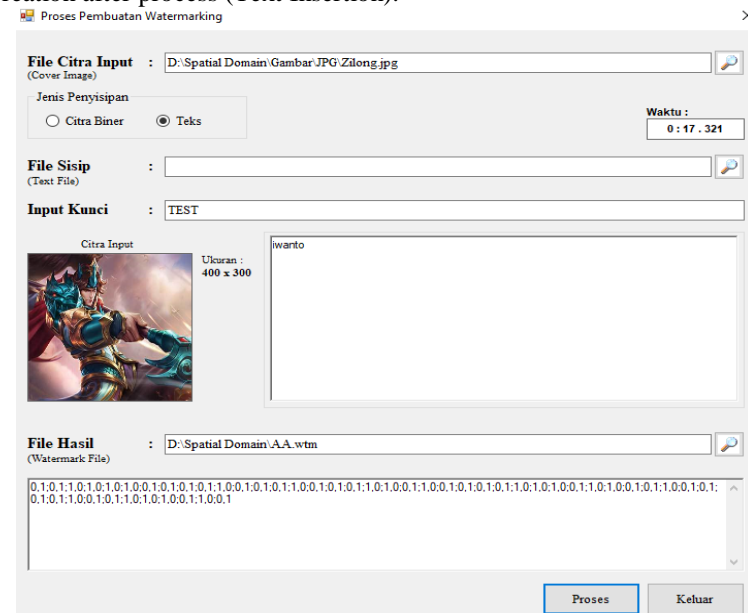


Fig. 6 Watermarking creation view after process (text insertion)

3. Watermarking check of extraction process (Insertion Of Binary Images).

\* Corresponding author



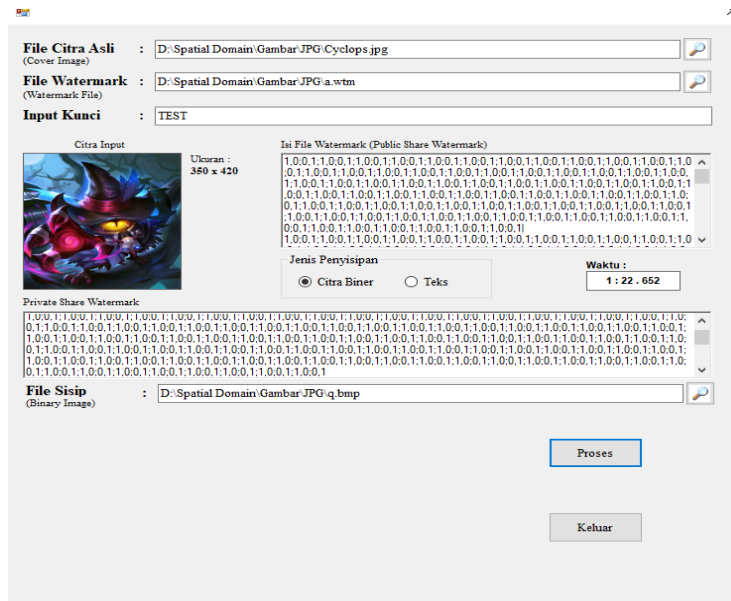


Fig. 7 Watermarking Check View Extraction Process (Binary Image Insertion)

4. Watermarking check after extraction process (Text Insertion).

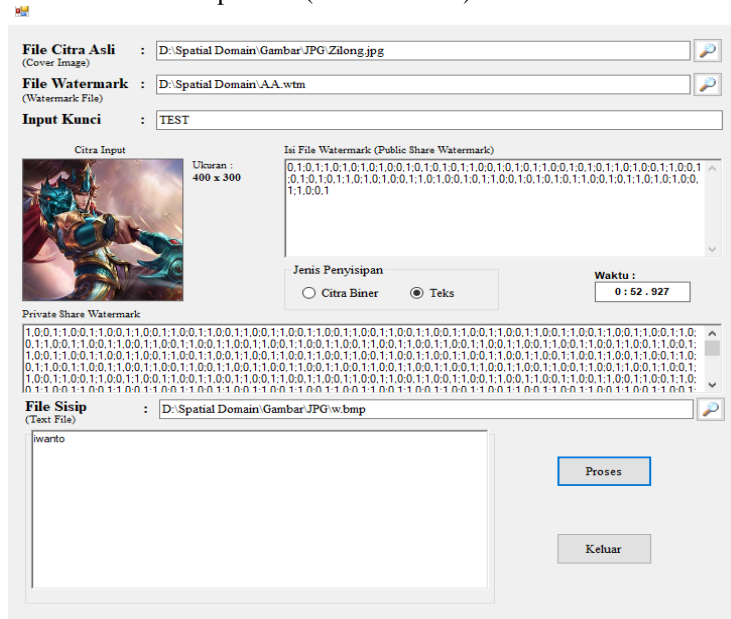


Fig. 8 Watermarking Check View After Extraction Process (Text Insertion)

5. Image comparison results.

\* Corresponding author



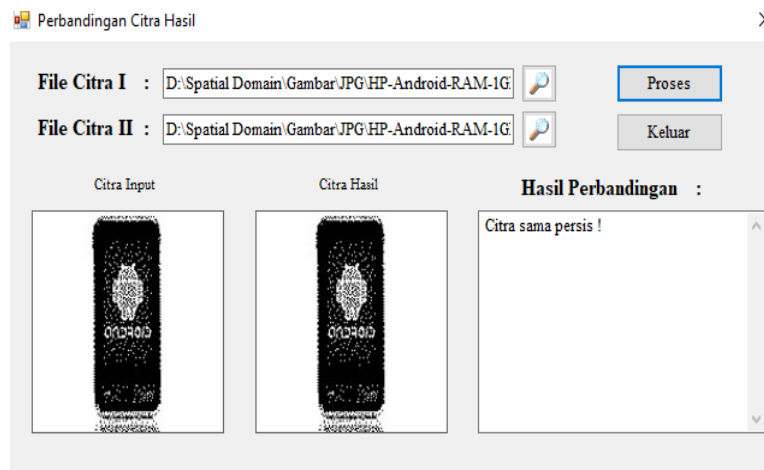




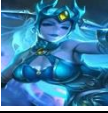

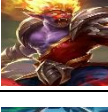

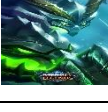



Fig. 9 Comparison After Image Comparison Process

Based on the test results of several images with a *spatial domain public image watermarkingscheme*, presented in table 2. Here:

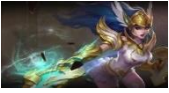












Table 1  
Image Testing Results

No	Original Image	Size	Image Format	Image Input	Size	Duration ( m : s )
1		350 x 420	JPG		150 x 150	0 : 11.649
2		400 x 300	JPG		150 x 150	0 : 14.262
3		240 x 390	GIF		150 x 150	0 : 7.593
4		518 x 649	BMP		150 x 150	0 : 27.734
5		450 x 620	GIF		150 x 150	0 : 25.153

\* Corresponding author












No	Original Imagic	Size	Image Format	Imgae Input	Size	Duration ( m : s )
6		400 x 294	GIF		150 x 150	0 : 11.16
7		400 x 300	JPG	Plain Text File name: Sisip Text.txt; "Iwanto"	-	0 : 52.927
8		518 x 649	BMP	Plain Text File name: Sisip Text2.txt; "UNPRI"	-	1 : 45.400
9		400 x 294	GIF	Plain Text File name: Sisip Text3.txt; "Negara Kesatuan Republik Indonesia".	-	0 : 23.121
10		1280 x 720	BMP		50 x 75	1 : 45.381
11		1125 x 685	GIF		175 x 225	1 : 38.725
12		1158 x 669	JPG		268 x 375	1 : 58.964
13		1280 x 720	BMP	Plain Text File name: Sisip Text.txt; "Iwanto"	-	12 : 42.590
14		1125 x 685	GIF	Plain Text File name: Sisip Text2.txt; "UNPRI"	-	7 : 57.427

\* Corresponding author





No	Original Image	Size	Image Format	Image Input	Size	Duration ( m : s )
15		1158 x 669	JPG	Plain Text File name: Sisip Text3.txt; "Negara Kesatuan Republik Indonesia"	-	7 : 0.41
16		1920 x 1080	BMP		732 x 965	25 : 34.930
17		1920 x 1080	GIF		645 x 815	14 : 50.520
18		1920 x 1080	JPG		1125 x 815	48 : 44.29

### DISCUSSIONS

In the process of creating watermarking the inputted comb image file using black-and-white images. The process of creating watermarking takes a relatively short time while the process of extracting watermarking processing time depends on the size of the image file. Watermarking is not affixed to the original image so there is no pixel change in the original image and there will be no leakage of information from watermarking. The location of the comb image file and watermarking file can be determined manually by the user. The resulting comb image file(binary)is stored in a file with an extension\*. bmp. The view of the comparison process can show what percentage of the immency between the two images is compared. Of the several image tests conducted using imagery with three formats, namely: JPG with an average accuracy of 9:5,310 (42.15%), GIF with an average time of 8:27.207 (21.63%), and BMP with an average time of 5:2,989 (36.22%). Thus, the determination of the image format used is adjusted to the original image, so that it can perform time efficiency.

### CONCLUSION

After completing the creation of this software, the author can draw some conclusions as follows, first, Spatial Domain Public Image Watermarking scheme can be used to reduce or minimize the possibility of hijacking information of an image (illegal copyright) by creating watermarks for the desired image and proving ownership rights through the watermark checking process. Second, Digital watermarking algorithm can be used to add watermarking to the image and can prevent leakage of watermark information because the contents of watermarking are not affixed to the cover image, but are generated on a separate file.

### REFERENCES

- Adi Suheryadi, (2017), Penerapan Digital Watermark Sebagai Validasi Keabsahan Gambar Digital Dengan Skema Blind Watermark, *Jurnal Teknologi Terapan*, Vol 3, No 2, ISSN 2477-3506.
- Ahmadi, S. B. B., Zhang, G., Rabbani, M., Boukela, L., & Jelodar, H. (2021). An intelligent and blind dual color image watermarking for authentication and copyright protection. *Applied Intelligence*, 51(3), 1701-1732.
- Alfred T., Ronal F. S., Setia B., Steven T. (2016), Aplikasi Perlindungan Hak Cipta Digital dengan Kriptografi dan Stenografi, *TEKNOMATIKA*, Vol.06, No.02, E-ISSN: 2541-335X.

\* Corresponding author



- B Surekha, Dr GN Swamy, (2016), A Spatial Domain Public Image Watermarking, *International Journal of Security and Its Applications*, Vol. 5 No. 1.
- Dwi E.K., Nanda R.H., Purwono P., (2018), Analisis Hasil Teknik Penyembunyian Hak Cipta Menggunakan Transformasi DCT Dan RSPPMC Pada Jejaring Sosial, *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIK)*, Vol. 5, No. 3, e-ISSN: 2528-6579.
- Ernawan, F. (2019). Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection. *International Journal of Electrical and Computer Engineering*, 9(3), 1850.
- Evsutin, O., & Dzhnashia, K. (2022). Watermarking schemes for digital images: Robustness overview. *Signal Processing: Image Communication*, 100, 116523.
- Farah S.I., Rizky R.J., Eka F.R., (2020), Digital Signature Menggunakan Metode Spread Spectrum Sebagai Perlindungan Hak Cipta Pada Citra Digital Mpeg-4, *JATIKOM*, Vol. 3 No. 1.
- Gangadhar, Y., Giridhar Akula, V. S., & Reddy, P. C. (2018). An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation. *Biomedical Signal Processing and Control*, 43, 31–40.
- Nuniek Herawati, (2019), Teknik Watermarking Menggunakan Metode CRT Pada deteksi tepi canny Untuk Perlindungan Hak Cipta (Dagadu), *Jurnal Teknologi Technoscintia*, Vol. 11No. 2, ISSN: 1979-8415.
- Ondi A., Dedy R. S., (2021), Pengamanan Hak Cipta Citra Digital Dengan Teknik Watermarking Menggunakan Metode Hybrid SVD Dengan DWT, *Jurnal Syntax Admiration*, Vol. 2 No. 11, e-ISSN : 2722-5356.
- Shaik, A., & Masilamani, V. (2021). A novel digital watermarking scheme using dragonfly optimizer in transform domain. *Computers & Electrical Engineering*, 90, 106923.
- Sheila R.F., Dyah C.I, (2016), Implementasi Digital Watermarking Pada Citra Menggunakan Metode Least Significant Bit, *Jurnal Informatika dan Komputer*, Vol 21 No. 3.
- Sisaudia, V., & Vishwakarma, V. P. (2021). Copyright protection using KELM-PSO based multi-spectral image watermarking in DCT domain with local texture information based selection. *Multimedia Tools and Applications*, 80(6), 8667-8688.
- Susanto, A., Sari, C. A., & Rachmawanto, E. H. (2017). Perlindungan Hak Cipta Pada Citra Digital Menggunakan Least Significant Bit Berbasis Deteksi Tepi Canny. *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, 8(2), 441-448.
- Wasilah., Suhendro I., Dona Y., (2016), Watermarking untuk Proteksi Hak Cipta Artifact dan Signature Menggunakan Metode CBIR, *Seminar Nasional Ilmu Komputer (SNIK 2016)*, ISBN: 9786021034408, hal 81-84.
- Zebua, T., Ndruru, E, (2017). Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4. *Jurnal Teknologi Informasi dan Ilmu Komputer*; Vol 4, No 4, e-ISSN: 2528-6579.

\* Corresponding author



This is an Creative Commons License This work is licensed under a  
Creative Commons Attribution-NoDerivatives 4.0 International License.