Improved Robust Image Watermarking with Polar Harmonic Transform Against Translation Attack

Mohamad Hanifan
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
hanifanmohamad@gmail.com

Rinaldi Munir
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
rinaldi.munir@itb.ac.com

***Abstract*— The use of polar harmonic transform for robust image watermarking has been developed since around 2012. Robust image watermarking which uses radial-based transformations becomes robust against rotational and scaling attacks. It generally uses the image center point as a reference for transformation. Thus, the type of attack such as translation which causes the image center point to change cannot be overcome. In this study, ORB Feature matching will be used to calculate the position of the reference point used during the embedding process, so that the embedding and extraction processes use the same point.**

The test results show that without the proposed method, a translation of 3 pixels can cause watermark damage as much as 30%. This proposed method can calculate the center point of the transformation accurately as long as the portion of the image lost due to translation is less than 43%. In the translation range of 12% in the vertical and horizontal directions, with this proposed method the number of damaged information bits drops from about 30% to 10% for the translation type which causes part of the image to be lost, and 0% for the translation type without causing part of the image to become lost.

Keywords—feature matching, image processing and computer vision, polar harmonic transform , robust image watermarking

I. Introduction

Technological developments have gradually changed the way of life of humans, one of which is the way of accessing information, both for work and entertainment. Nowadays people prefer to upload photos to social media rather than stored in memorable albums. The fast development of technology has made people prefer to exchange information online because it is considered more practical.

Unfortunately, technology advancement develops crime too. Dissemination of information online invites piracy, aided by the abuse of editing technology. One type of data that is often targeted is digital images. Once the image is uploaded to social media or other online platforms, others can easily download or re-upload it without mentioning the ownership information.

One method of authorizing digital image ownership to prevent piracy is watermarking. This method is done by inserting certain information that can be used to identify the owner of the image. In research that has been widely publicized, watermarks that are inserted are binary images in the form of logos.

In general, there are 2 types of watermarking, each of which has a different function, namely 1) Fragile Watermarking, a watermark embedding method that will be damaged if the image undergoes editing, and 2) Robust Watermarking, a watermark insertion method that will not be damaged even though the image is edited. In this study, we wish that the inserted watermark can be extracted again and should not be damaged even though the image has been edited so that the method used is Robust Watermarking. Also, because this research focuses on the case of digital images, more specifically the method to be used is called Robust Image Watermarking.

In Robust Image Watermarking (RIW), there are 3 main factors of concern [11], 1) robustness, the level of resilience of the information in the image against the editing that occurs, and it can be measured from the number of bits of information that changes, 2) imperceptibility, the level of image similarity between before and after insertion, and 3) capacity, indicating how much information can be inserted into the image.

Based on how to extract watermarks, Robust Image Watermarking (RIW) is divided into blind and non-blind [11]. The non-blind watermarking method requires the original image to extract, whereas in the blind watermarking the extraction process can be done without the original image. The method proposed in this study is a non-blind method.

Editing that occurs on watermark images is generally referred to as attack because it is considered to attack the existence of the inserted information. Types of editing commonly tested in research are signal processing attacks and geometric attacks. Signal processing attacks are edits that cause changes in pixel values in an image, for example, smoothing or noise. Meanwhile, geometric attacks are edits that cause changes in pixel position, for example, rotation, translation, and scaling.

Robust image watermarking with polar harmonic transform has a good performance against both signal processing and geometric attack, except for translation. Polar harmonic transform uses a reference point for transformation, which usually uses the center point of the image. Any attacks that move the position of that point causes the embedding and extraction process unsynchronized. Those processes will use different reference point and the transformations give a different result.

In this research, we propose a mechanism to calculate the reference point used in the embedding process before extracting the watermark. The calculation will be done by taking into account the matching feature between the watermarked image and the translated image. Feature matching will use Oriented fast and rotated brief (ORB) as the feature detector [7]. That way, the extraction process can use the same reference point as the embedding process.

II. RELATED WORKS

Robust Image Watermarking method which is quite popular to use is namely Discrete Cosine Transform as in [5]. The image is divided into 8x8 pixel small blocks and then transformed into the frequency domain using DCT. Watermark is inserted into the frequency domain because it can increase robustness. The drawback of this method is that it cannot overcome geometric attacks.

In 2010, Yap [1] introduced the Polar Harmonic Transform (PHT). PHT is the transformation of the spatial domain into a set of moments based on radially and invariant to rotation and magnitude. PHT allows the development of a robust RIW method against geometric attacks.

Leida, Shushang, Ajith, and Jeng-Shyang [2] in 2012 used PHT to carry out watermarking by first selecting accurate moments as insertion media. This research produces a watermarking method that is not only robust against signal processing attacks, but also for rotation and scaling.

Then Hosny and Darwish [3] in 2017 and Hongcai, Xiaobing, Yajun, and Yilan [4] in 2019 developed Leida's research, and produce a method that has better robustness and imperceptibility than before. However, all three studies cannot overcome this type of translational editing.

III. POLAR HARMONIC TRANSFORM

One of the approaches used when embedding watermarks in robust image watermarking is the polar harmonic transform (PHT). In this approach, the image will be transformed from a spatial domain into a set of radial based moments. Polar harmonic transform (PHT) [1] is a group consisting of polar complex exponential transform (PCET), polar cosine transform (PCT), and polar sine transform (PST). In general, the PHT equation is shown in (1).

$$M_{nl} = \frac{1}{\pi}\int_0^{2\pi}\int_0^1 [H_{nl}(r,\theta)]^* \cdot f(r,\theta) \cdot r \cdot dr \cdot d\theta \qquad (1)$$

The function H$_{nl}$ (r, θ) can be translated into radial and circular components as shown in (2).

$$H_{nl}(r,\theta) = R_n(r)e^{il\theta} \qquad (2)$$

The difference between PCET, PCT and PST lies in the radial kernel component. (3), (4), and (5) show the kernels for PCET, PCT, and PST respectively.

$$R_n(r) = e^{i2\pi nr^2} \qquad (3)$$

$$R_n^C(r) = \cos(\pi nr^2) \qquad (4)$$

$$R_n^S(r) = \sin(\pi nr^2) \qquad (5)$$

The three transformations fulfill the orthogonal conditions in (6).

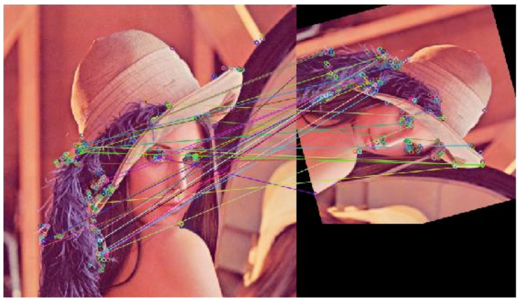

Figure 1. Feature matching between original image and rotated image

$$\int_0^{2\pi}\int_0^1 H_{nl}(r,\theta)[H_{n'l'}(r,\theta)]^* r dr d\theta = \pi\delta_{nn'}\delta_{ll'} \qquad (6)$$

The image that is transformed using PHT in (7) produces a set of moments that are invariant to rotation and magnification. Therefore, the robust image watermarking algorithm which is based on PHT is also robust against both types of editing. Equation (8) is used to transform the moment back into the spatial domain.

$$\begin{gathered} M_{nl} = \frac{4}{\pi N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}[H_{nl}(r,\theta)]^* \cdot f(i,j) \\ r = \sqrt{x^2+y^2} \text{ dan } \theta = \tan^{-1}\frac{y}{x} \\ x = \frac{2i-N+1}{N} \text{ dan } y = \frac{2j-N+1}{N} \end{gathered} \qquad (7)$$

$$f(r,\theta) = \sum_{n=-\infty}^{\infty}\sum_{l=-\infty}^{\infty} M_{nl}H_{nl}(r,\theta) \qquad (8)$$

IV. ORB FEATURE MATCHING

ORB (Oriented FAST and Rotated BRIEF) is a method to search for features in images and free. ORB developed in 2011 [7] by integrating the keypoint detection method FAST and BRIEF descriptor. ORB has an advantage in terms of speed versus other methods such as SIFT. This method is also robust against rotation. An example of feature matching between an original image with the rotated version is shown in Figure 1.

In this research, ORB will be used to find the features of the image before and after editing. The features of both images will be matched against each other to calculate the position of the image's center point relative to these features.

The figure shows the result of feature matching between images before and after undergoing geometric editing.

V. Watermarking Scheme

A. Embedding Process

Watermark insertion into the image is carried out in the transformation domain by manipulating the moment magnitude. The steps for performing the insertion are as follows:

1. The image used in this study has a PNG extension and is square in size NxN, while the watermark used is GxG in binary format.
2. From the RGB color space, the image is converted to the YCbCr color space because the insertion will be carried out to the Y channel.
3. The Y channel portion is transformed using PHT so that it is generated a set of moments (M_{nl}) with the maximum moment value P, so that satisfies $|n| + |l| \leq P$, where the center of the transformation is a point $O(\frac{N+1}{2}, \frac{N+1}{2})$.
4. Of all the available moments, not all will be used for insertion. The moment to be used is the accurate moment that has positive order and the repetition is not a multiple of 4, $\{M_{nl}, n > 0, l \neq 4m, m \in Z\}$.

$$M'_{nl} = \begin{cases} 2\Delta \cdot \left[\frac{|M_{nl}|}{2\Delta}\right] + \frac{\Delta}{2}, jika\ w = 1 \\ 2\Delta \cdot \left[\frac{|M_{nl}|}{2\Delta}\right] - \frac{\Delta}{2}, jika\ w = 0 \end{cases} \tag{9}$$

$$\omega = \frac{M'_{nl} - |M_{nl}|}{|M_{nl}|} \cdot M_{nl} \tag{10}$$

5. Watermark is inserted by manipulating the moment value based on (9). The notation Δ indicates the quantization step, notation $[\cdot]$ represents a rounding operation to the nearest unit, and the notation $|\cdot|$ indicates magnitudes of a complex number.
6. Compensation image is formed by the inverse transformation of PHT on moment of modification ω from (10).
7. The insertion process is done by combining the Y channel from the original image with a compensation image, resulting in a Y channel with a watermark, (Y ').
8. The Y' channel is combined with the Cb and Cr channels from the original image to produce a watermarked image in the YCbCr color space. Image with a watermark then converted into RGB color space.

B. CalculattingReference Point

Before the extraction process begins, to overcome translation we have to calculate the reference point used by the embedding process. This calculation process includes non-blind watermarking.

The steps in the center point calculation process are as follows:

1. The process of calculating the center of rotation is done by taking the features from the image before undergoing editing and after undergoing editing. Feature selection is done using the ORB method.
2. The features of the image before and after being edited are matched using a brute force matcher, until a collection of feature pairs from both images is obtained, $\{F(x,\ y,\ x',\ y')\}$, where F is the feature pair located at coordinates (x, y) in the image before undergoing editing and coordinates (x', y') in the image after undergoing editing. In the calculation, only the F feature pair of nF is used with the highest match value with a value of n equal to 50.
3. The transformation center point in the image before undergoing editing is $(c_x, c_y) = (\frac{N+1}{2}, \frac{N+1}{2})$, while the initial estimate of the transformation center point in the image after editing is $(c'_x, c'_y) = (\frac{N'+1}{2}, \frac{N'+1}{2})$, where N' is the size of the image after editing.
4. The error (ε) of determining the position is calculated by (11). Then the c_x', c_y' and s parameters are optimized to get the minimum ε value.

$$\varepsilon = \sum_{i=1}^{nF} (r_i - s \cdot r'_i),$$

$$\text{where } r = \sqrt{(x - c_x)^2 + \left(y - c_y\right)^2}, \text{ and } r' = \sqrt{(x' - c'_x)^2 + \left(y' - c'_y\right)^2} \tag{11}$$

C. Extraction Process

The watermark extraction process is the opposite of the insertion process. The steps in the extraction process are as follows:

1. From the RGB color space, the image is converted to the YCbCr color space.
2. The Y channel portion is transformed using PHT so that it is generated a set of moments (M_{nl}) with the maximum moment value P, so that satisfies $|n| + |l| \leq P$, where the center of the transformation is a point $O(\frac{N+1}{2}, \frac{N+1}{2})$.
3. From all available moments, accurate moments used in the insertion are selected which have positive order and the repetition is not a multiple of 4, $\{M_{nl}, n > 0, l \neq 4m, m \in Z\}$.

$$w = \begin{cases} 0, jika\ M_{nl} - 2\Delta \cdot \left[\frac{|M_{nl}|}{2\Delta}\right] < 0 \\ 1, jika\ M_{nl} - 2\Delta \cdot \left[\frac{|M_{nl}|}{2\Delta}\right] > 0 \end{cases} \tag{12}$$

4. The watermark information is extracted from the moment using (12).
5. Watermark is formed by arranging the obtained bits into a binary image with the GxG size.

VI. Test Results

The translation editing test is carried out by extracting the watermark from the translated image towards the x-axis and y-axis. In this test, 2 types of translation were carried out as shown in Figure 2, namely translation with crop and translation without crop. In translation with crop, the image will be cropped because the size before and after editing remains the same. Whereas in the translation without crop, there is no cropped image, but the image size becomes larger.

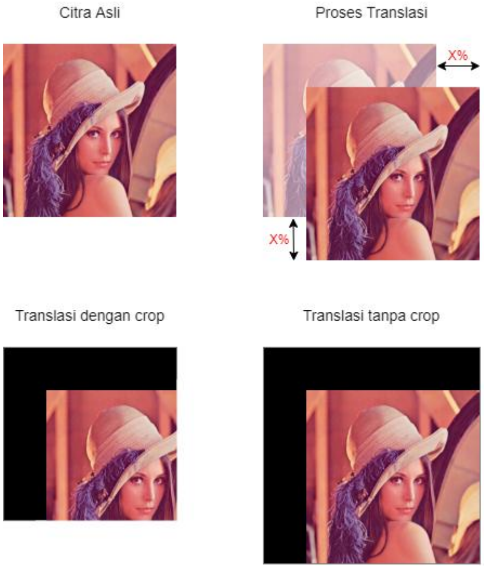

Figure 2 Image Translation

If the watermark is directly extracted from an image that has undergone translation editing, the transformation at the time of insertion and extraction will use a different center point, so that the radius (r) and angle (θ) values are different. This will result in a major damage to the watermark, as shown in Figure 3. It can be seen that the translation of just 3 pixels can cause the BER value to be above 20%. The graph also shows that for small translations (less than 3 pixels), the larger the image size causes the translation to be more robust.

Figure 4 shows the error rate in the calculation of the center point of the transformation to the amount of translation that occurs in the image. For a translation of x%, the test is carried out by translating by cropping the image with a random quantity of (x-0.05)% <translation <x%. For each value, the test was carried out 10 times and the average was taken.

Table 1 Testing parameter for translation attack

Image Size (N)	512
Watermark Size (G)	20
Maximum Momen (P)	40
Quantization Step (Δ)	0.3

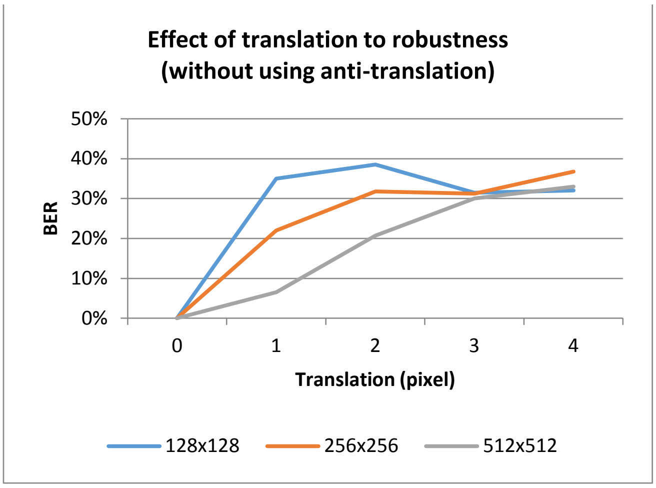

Figure 3 Effect of image size to translation

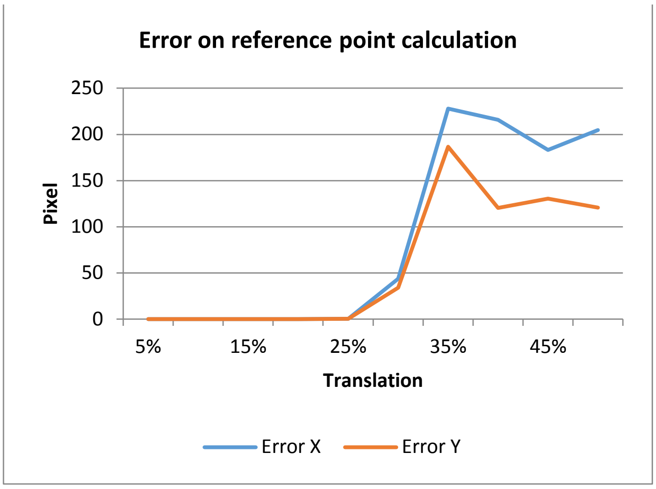

Figure 4 Image translation and calculation error

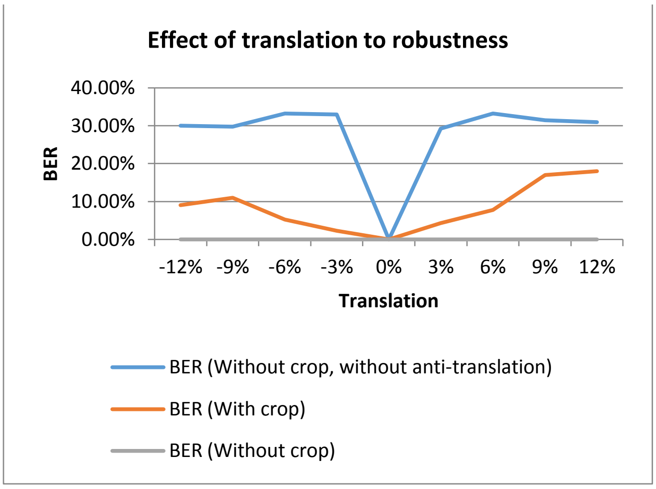

Figure 5 Translation testing results

The test results showed that the calculation error increased dramatically after the image was translated to the x and y axes by more than 25%. This occurs because the calculation of the translation center point is carried out using feature matching, so that the more parts of the image are lost, the more features are lost, so that the feature matching process becomes less accurate.

Table 1 shows the parameters used to perform translation testing. The test results are shown in Figure 5. From these results, it can be seen that for translation with crop, the greater the translation that occurs causes less robustness. This is due to the missing data due to the editing process, so that the transformation process produces different values. In addition, the loss of data also causes the feature matching process to be inaccurate, resulting in errors in calculating the position of the transformation center. Meanwhile, for translation editing without crop, the BER value remains at 0. This means that this type of editing can be resolved by the proposed method.

Final test shown in Figure 6. It is used image size 512x512, watermark size 20x20, quantization step 0.2. The embedding process give 37.15. From the attack process, the BER value doesn't pass more than 10%. The biggest error is for the translation attack with anti-translation 9.25%, and the second biggest is crop 6.5%.

VII. CONCLUSION

The proposed robust watermarking performance is proven to be superior in overcoming translation editing. For a translation range of -12% to 12%, the BER value drops from about 30% to about 10% for translation types with crop and 0% for translation types without crop. The weakness of the method in this study is the imperceptibility factor, seen from the PSNR value which is still below 40.

REFERENCES

[1] P.T Yap, X. Jiang, Alex C. Kot, "Two-Dimensional Polar Harmonic Transforms for Invariant Image Representation," 2010

[2] Leida L., Shushang Li, Ajith A., JS Pan, "Geometrically invariant image watermarking using Polar Harmonic Transforms," 2012

[3] Khalid M. Hosny, M. M. Darwish, "Invariant image watermarking using accurate Polar Harmonic Transforms," 2017

[4] Hongcai Xu, Xiaobing Kang, Yajun Chen, Yilan Wang, "Rotation and scale invariant image watermarking based on polar harmonic transforms," 2019

[5] Soumitra Roy, Arup Kumar Pal, "A blind DCT based color watermarking algorithm for embedding multiple watermarks," 2017

[6] Samir S. Soliman, Mandyam D. Srinath, "Continuous And Discrete Signals And Systems," 1990

[7] Ethan Rublee, Vincent Rabaud, Kurt Konolige, Gary Bradski, "ORB: An efficient alternative to SURF or SIFT," 2011

[8] X.Y. Wang, Y.N. Liu, S. Li, H.Y. Yang, P.P. Niu, "Robust image watermarking approach using polar harmonic transforms based geometric correction," 2016

[9] Chandan Singh, Amandeep Kaur, "Fast computation of polar harmonic transform," 2012

[10] Junliu Zhong and Yanfen Gan, "Discrete Polar Complex Exponential Transform for Image Rotation Duplication Detection", 2015

[11] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques," 2005

[12] Ismail A. Ismail, Mohamed A. Shouman, Khalid M. Hosny and Hayam M. Abdel Salam, "Invariant Image Watermarking Using Accurate Zernike Moments," 2010

[13] E. Najafi, K. Loukhaokha, "Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform," 2018

[14] Yang Hong-Ying, Wang Xiang-Yang, Wang Pei, Niu Pan-Pan, "Geometrically resilient digital watermarking scheme based on radial harmonic Fourier moments magnitude," 2014

[15] Zhang Wuyonga, Chen Jianhuaa, Zhang Yufeng, " Global resynchronization-based image watermarking resilient to geometric attacks," 2018

[16] Saeid Fazli, Masoumeh Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," 2016

[17] Manuel Cedillo-Hernández, Francisco García-Ugalde, Mariko Nakano-Miyatake, Héctor Manuel Pérez-Meana, "Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification," 2013

[18] Chang CC, Tsai P, Lin CC, "SVD-based digital image watermarking scheme," 2005

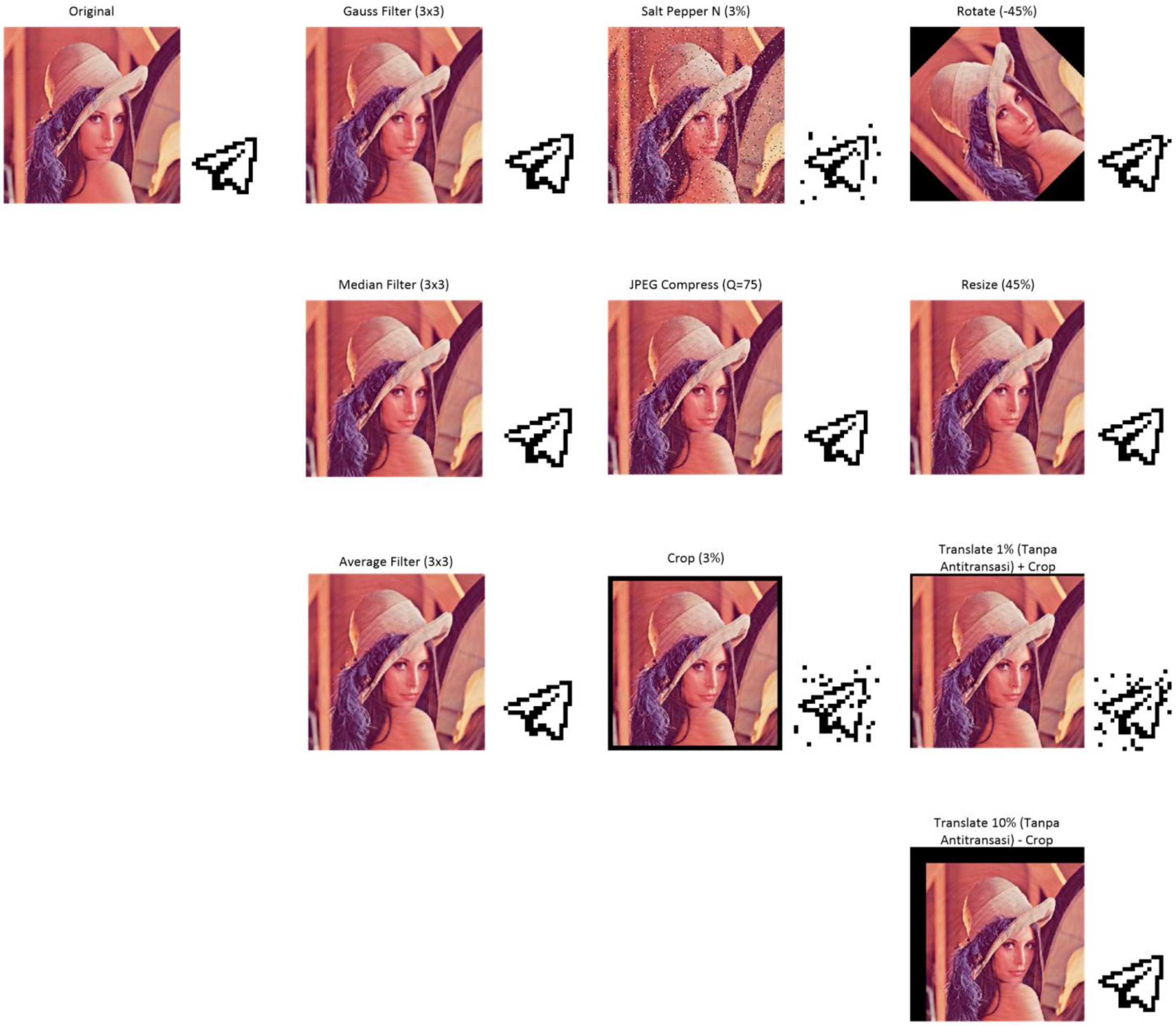

Figure 6 Testing results against signal processing and geometric attacks