A New Copyright Protection for Vector Map using FFT-based Watermarking

Shelvie Nidya Neyman*[1], I Nyoman Prama Pradnyana[2], Benhard Sitohang[3]
School of Electrical Engineering and Informatics (STEI) - ITB
Ged. Achmad Bakrie Lt. 2Jl. Ganesha No 10, Bandung, Indonesia,
Telp. +62-22-2502260, Fax. +62-22-2534222
*Corresponding author, e-mail: shelvie@ipb.ac.id[1], prama.pradnyana@itb.ac.id[2], benhard@stei.itb.ac.id[3]

Abstract

This study proposed a new approach of copyright protection for vector map using robust watermarking on FFT algorithm. A copyright marker inserted in vector map as the watermark. In addition to data origin authentication capabilities watermark, RSA cryptographic algorithm is used when generating the watermark. Quality measurement of the results was based on the three characteristics of digital watermarking: (1) invisibility using RMSE calculations, (2) fidelity with the farthest distance and (3) NC calculation and gemotrical level of robustness against attacks. Result of experiments showed that the approach used in this study succeeded in inserting copyright as watermark on vector maps. Invisibility test showed good results, demonstrated by RMSE close to zero. Fidelity of the watermarked map was also maintained. Level of watermark robustness against geometric attacks on vector map results has been maintained within the limits that these attacks do not affect the watermark bit value directly.

Keywords: copyright protection, vector map, robust watermarking, fast Fourier transform (FFT)

1. Introduction

Over the past few decades, geospatial data production process has evolved from paper maps to digital data format because of the influence of the development of computer technology for geographic data collection devices such as geographic positioning systems (GPS) and satellites that provide accurate spatial coordinate data.Vector maps as the fundamental data of a geographic information system (GIS) has replaced the role of analog data or print [1] . This is understandable because geospatial vector data has the advantage of high precision data, automated processes and lossless scaling compared to the data in paper form. Easier production, storage and distribution in digital maps transaction brings about other consequences, namely easy manipulation and acquisition. It encouraged a need among the map producers for a map production mechanism that can facilitate copy right marker [2].Furthermore, map consumersalso require the ability to know the ownership identity of the spatial data they receive.In addition, regulatorshave the need to verify the validity of the publicly distributed map ownership.Digital watermarking is one of the best solutions that can be utilized to solve the problem.

Digital watermarkingis a technique that works by inserting certain information (referred as watermark) into a digital media file, when used on a digital map, the information may contain data which is used to verify the integrity or ownership of the map; provided that the insertion process should result in very small distortion value of the resulting map[3]. Robust digital watermarking is one of digital watermarking techniques that has resistance characteristic toward data contents removal and modification when its insertion media point changes, either due to attacks or data processing. During application stage, this technique is commonly used for copyright protection. The application of robust digital watermarking techniques on map vector works on two types of domains; spatial domain and transformation domain [3]. The main transform algorithms are DFT (*Discrete Fourier Transform*), DWT (*Discrete Wavelet Transform*), and DCT (*Discrete Cosine Transform*) [4]. These digital watermarkings in the transformation domain are known to be robust to attack. Fordigital mediacopyright protection application, robust digital watermarking technique mainly work on the transformation domain; because the transformation domain has some advantages in terms of invisibility and strong robustness, compared with the spatial domain which have fragile nature, and implementation ease [5].

At present, researchers mostly concentrate on the robust digital watermarking algorithm in transformation domain for image[6]-[11], and audio[12]-[16]. Characteristics file vector map is very different from the image or audio as watermark embedding media.For it takes a different technique for inserting a information in the vector map. Some existing research has proposed the use of robust digital watermarking onthe transformation domain of vector map using data transformation algorithms based upon DFT [2], IWT (Integer Wavelet Transform) [17], and DCT[18]-[20]. Only two existing studies that were specifically carried out for the purposes of vector map copyright protection [2],[17]. Other research studies that discuss the topic of copyright digital maps with different techniques are blind watermarking with DCT [21], zero watermarking in the spatial domain [22], recursive watermarking in spatial domain [23], watermarking in spatial toplogy domain [24], and reversible watermarking in spatial domain [25].

To enhance copyright protection performance techniques on vector maps, this study proposes the use of robust digital watermarking domain transformation as proof of copyright on vector map using FFT data transformation algorithm.FFT algorithm is very popular in the watermarking community [26] and never used to vector map as embedded media. FFT often used due to its reduced computational burden while maintaining the quality of insertion compared with some other data transformation algorithms [27]. In addition to ownership marking purpose, the approach taken in this study also provides data origin authentication capabilities via the RSA public key cryptography algorithm.With the use of the algorithm, data origin authentication can obtained security through ownership private key used to encrypt copyright on vector maps.User can easily to authenticate data origin of the map by using RSA public key.

The performance techique is measured through similarity test using NC calculation. The test is used to determine the success of this technique in the insertion of copyright into a vector map. The results of this study measured objectively, not based on perception as on some existing research[17],[18],[28].Quality measurement of the results of this study was based on three of the characteristics of digital watermarking. They areinvisibility using root mean squared error (RMSE)calculations, fidelity with the farthest distance calculation, and normalized cross correlation (NC), and the strength of watermark robustness against gemotrical attacks such as translation, rotation and scaling [29].

The result findings showed that the approach used in this study succeeded in inserting copyright as watermark on vector maps. Invisibility on the experimental result findings showed good results, demonstrated by RMSE values generated from the map test data values: below 1 or close to zero. Fidelity of the map is also maintained, indicated by the distance shift and NC values in the range deemed acceptable according to standards. Level of watermark robustness against geometric attacks on vector map results has been maintained within the limits that these attacks do not affect the watermark bit value directly or still within the specified value extraction limits.

In the next part of this paper we will explain the techniques used on the approach developed in this study, followed by an elaboration of the experimental results and analyses of the performance of the approach. The final section of this paper closes with conclusions.

2. Research Method
2.1. Fast Fourier Transform

Fast Fourier Transform (FFT) is an algorithm used to represent a signal in a discrete time and a frequency domain. FFT in general is used to calculate the discrete transformation of the DFT quickly and efficiently. FFT is used to decrease the complexities of the DFT. Generally, the FFT formulation can be described as it is in the equation (1) or (3) [30].

$$H(k) = \sum_{n=0}^{N-1} h(n)\, W_N^{nk} \qquad (1)$$

$$W_N = e^{-j2\pi/N} = cos(2\pi/N) - j\ sin(2\pi/N) \qquad (2)$$

$$H(k) = \sum_{n=0}^{(N/2)-1} h(2n)\, W_{N/2}^{nk} + \sum_{n=0}^{(N/2)-1} h(2n+1) \tag{3}$$

$H(k)$ is the domain transformation value, $h(n)$ is the digital media block value, N is the amount of the data that will be altered to be a frequency domain. While for the inverse formulation of the FFT is using the equation (4).

$$h(n) = \frac{1}{N}\sum_{n=0}^{N-1}[Re * cos\left(\frac{2\pi kn}{N}\right) + Im * sin\left(\frac{2\pi kn}{N}\right)] \tag{4}$$

Re is the real value of the complex figure, Im is the imaginary value of the complex figure, and $h(n)$ is the watermarked complex sequence value.

2.2. Transform Transform

In this research, the watermark insertion as a copyrights marker on the vector map is conducted on the transformation domain for the coordinate of vertices.The watermark insertion process is conducted on the coefficient of the transformation result frequency of the vector map data. To transform vector map into domain frequency signal, the vector map coordinate is modified into a complex sequence a_k with the formulation (5) [2].

$$a_k = x_k + y_k \tag{5}$$

x_k is the abscissa of the vector map coordinate and y_k is the ordinate of the vector map coordinate. While the k used is the coordinate index occurred in the map file mentioned. The technique used for the watermark insertion is this formula (6).

$$F' = F + \alpha W \tag{6}$$

F' is the watermarked frequency coefficient, F is the initial frequency coefficient, α is the modification amplitude, and W is the watermark bit. On the (6) formulation above, the bigger α used, the bigger changes will happen on the vector map file, but the watermark resistance is stronger. This research uses α value as big as 2, with an acceptable vector map changes, and a highresistance value[31].

2.3. The Embedding Watermark Phase

The embedded model of digital watermark of the vector map data is shown in Figure 1. In the watermark insertion process, three inputs are used. They are vector map, a copyright inserted in as the watermark, and the private key of the RSA cryptograph algorithm. The first stage of the insertion process is by looking for the coordinate on the vector map that will be saved into a list which can be transformed into a domain frequency. After getting a set of coordinate from the vertex point of each feature, that coordinate therefore will be transformed into a complex sequence. The next stage is the reading or the byte watermark from the copyright marker file and encrypted with an RSA private key algorithm of the copyright holder. The purpose of this encryption is to provide security for the data origin authenticity, which is a guarantee that the data source is from a legitimate party. The watermark encryption result then transformed into a bit set and saved into a list. After both inputs are ready, the next stage is to do the complex sequence saving and lengthen the byte watermark in a different file. Later, the complex sequence will be used to extract the watermark with the non-blind watermarking. The next step is transforming the FFT towards vector map file to become a frequency domain and the watermark insertion on the real result figures of the transformation domain mentioned. And after the entire watermark has been inserted, then the next step is to restore the frequency domain vector map to return to its original shape file with iFFT.

2.4. The Extracting Watermark Phase

The watermark extraction point is basically the same with the insertion process with a reverse steps. In the extraction process, we use the three inputs that are the results of the insertion process such as the complex sequence of the real vector map file, watermarked vector map, and RSA algorithm public key. You can see the stages of the watermark extraction on Figure 2.
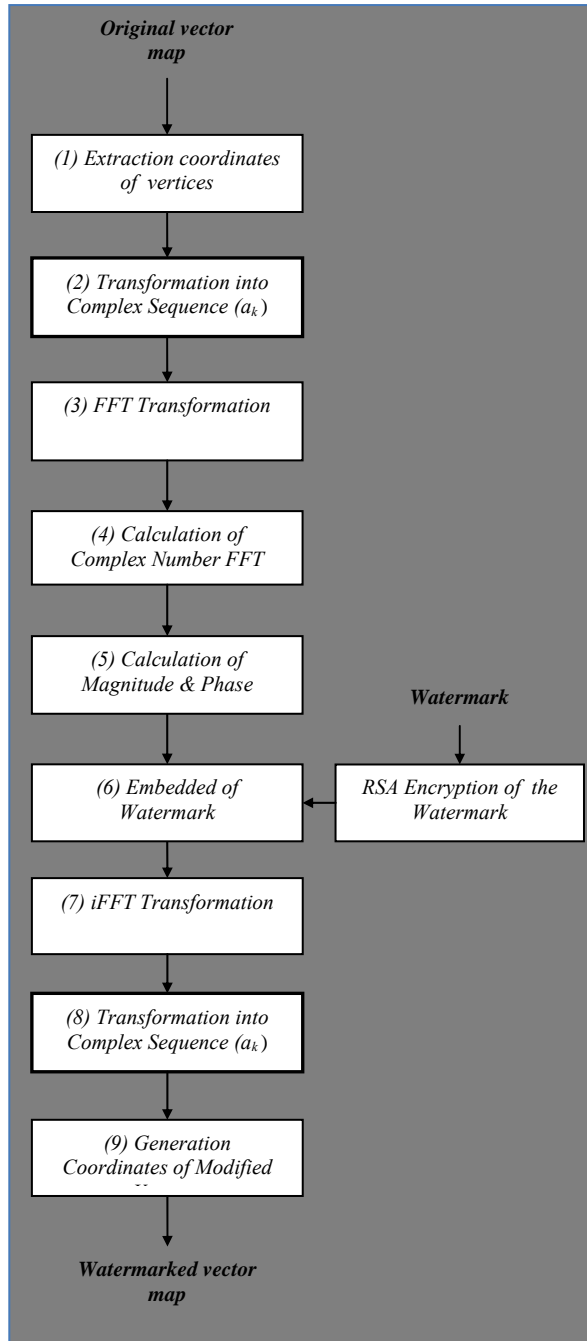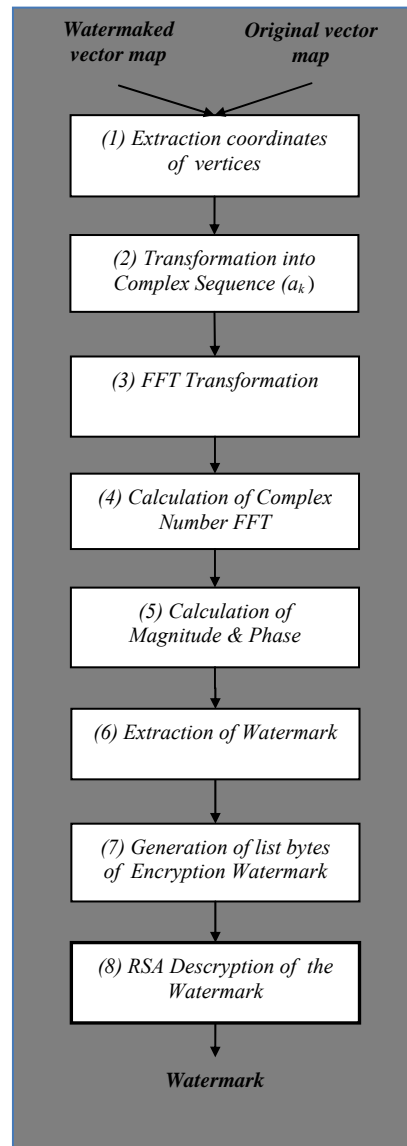

Figure 1. Watermark embedded

Figure 2. Watermark extracted phase

The first stage of the extraction process is to look for the coordinate from the shape file vector map that consists of watermark and save it in a list to be transform into a frequency domain. The next stage is to calculate the complex sequence and FFT to obtain the complex figure from the shapefile file. The list is consist of the encrypted watermark bit value gotten from the deviation of the complex figure from the real map and the watermarked map. Then, by using the the RSA public key, decrypt the watermark for the initial watermark as a copyright marker. The decryption process can be done when the encrypted watermark uses the right public and private key set, so we can assure that the copyright is from a legitimate party.

3. Results and Discussion
3.1. Experimental Results

Vector map used as the evaluation data is two shapefile (.shp) file type ESRI standard that was built from point features with 4008 vertex and line features with 7518 vertex. As a copyright marker, we used three bitmap type picture files with these measurements for each: 178 byte (29 x 29 pixels), 154 byte (22 x 23 pixel) and 174 byte (28 x 28 pixels). The length of the copyrights marker bit is limited to twice smaller than the vertex amount on the vector map file.

The performance technique analysis developed in this research was measured through NC calculation. The NC calculation was done to analyze the similarity between the initial watermark before the insertion and the extracted watermark result with the value ranging from 0 to 1. The higher the NC value, the more similar both images, therefore it can be stated that the watermarking usage technique success is higher. The NC calculation result used the equation (7) with w is the initial watermark and w' is the extracted watermark result that can be seen in Table 1 [2].

$$NC = \frac{|w \cdot w'|}{\sqrt{w \cdot w}\sqrt{w' \cdot w'}} \tag{7}$$

Table 1. Result of similarity test between original watermark with extracted watermark

Map	Size of Original Watermark (byte)	Original Watermark	Extracted Watermark	Size of Extracted Watermark (byte)	NC
Linestring	178			178	1
	154			154	1
	174			174	1
Point	178			178	1
	154			154	1
	174			174	1

Table 1 shows that the entire evaluation data results in NC is 1 with the same watermark length and content. Similarity value is equal to 1 between the initial watermark with the watermark extraction results show that both watermark identical. Watermark can be re-extracted from the vector map file and it will not go through size or content changes. Therefore, we can confirm that this technique succeeded in inserting copyrights as a watermark without changing the watermark quality.

3.2. Invisibility Evaluation

Invisibility measurement uses two parameters as reference analysis is the calculation of RMSE. The calculation of the distortion between the beginning of the map file and the result of interpolated watermark was conducted in the RMSE measurement. The RMSE formulation used is based on Equation (8) [32].

$$\text{RMSE} = \sqrt{\sum_{i=0}^{N}\sum_{j=0}^{N}\frac{[I(i,j)-I'(i,j)]^2}{[I(i,j)]^2}} \tag{8}$$

N denotes the number of vertex map vector, $I(i,j)$ is the value of complex sequence of early maps at coordinate (i,j), $I'(i,j)$ is the value of complex sequence of the map result at coordinate (i,j).

Table 2. Result of invisibility test between original map with watermarked map

Map	Watermark	Size of Watermark (byte)	RMSE
Linestring		178	0.00000005
		154	0.00000005
		174	0.00000005
Point		178	0.005115
		154	0.005115
		174	0.005201

Table 2 shows that the RMSE values obtained for all data analysis used in this research produces a value below 1 and close to zero. The results of this study show an improvement compared to previous similar study[4].Therefore, the techniques used to generate a good RMSE data analysis output value indicates that the occurrence of geometrical distortion scale, due to the copyright marking on the map, is very low. The low distortion shows that the presence of a watermark on media interpolation is difficult to be detected by the human senses.

Figure 3 show result of the overlay the original map and corresponding watermarked map using red dottes and purple dottes. Green box marks a shift in the coordinates of the vertex of the two maps. The figure can be viewed that the distorsion caused by watermark embedding process is small enough and the watermarked map preserveves the geospatial information in the original map with high precision.

3.3. Fidelity Evaluation

The fidelity aspect of digital watermarking concept is defined as the watermark cannot be detected by human senses and does not significantly degrade the quality of the media file interpolation [31]. Besides RMSE, farthest changes occurred will also be measured. Farthest distance is a position shift that occurs due to the watermark interpolation into the vector map files. The farthest distance is obtained by comparing the entire coordinate's vertex between original vector map file and vector map file containing watermark. Farthest distance is then converted into meter using Quantum software GIS. According to the Geographical Survey Institute of Japan, the changes that can be tolerated is equal to 75 cm on the actual size [31]. Based on Table 3, visible shift in the longest position occurred in the data analysis is equal to

0.506 meters by 51 cm, or in other words, the changes that occurred is not more than 75cm. In this case, the calculation result of the farthest distance value applied to the data analysis can still maintain a level of vector map precision or preserve accuracy level of the data.
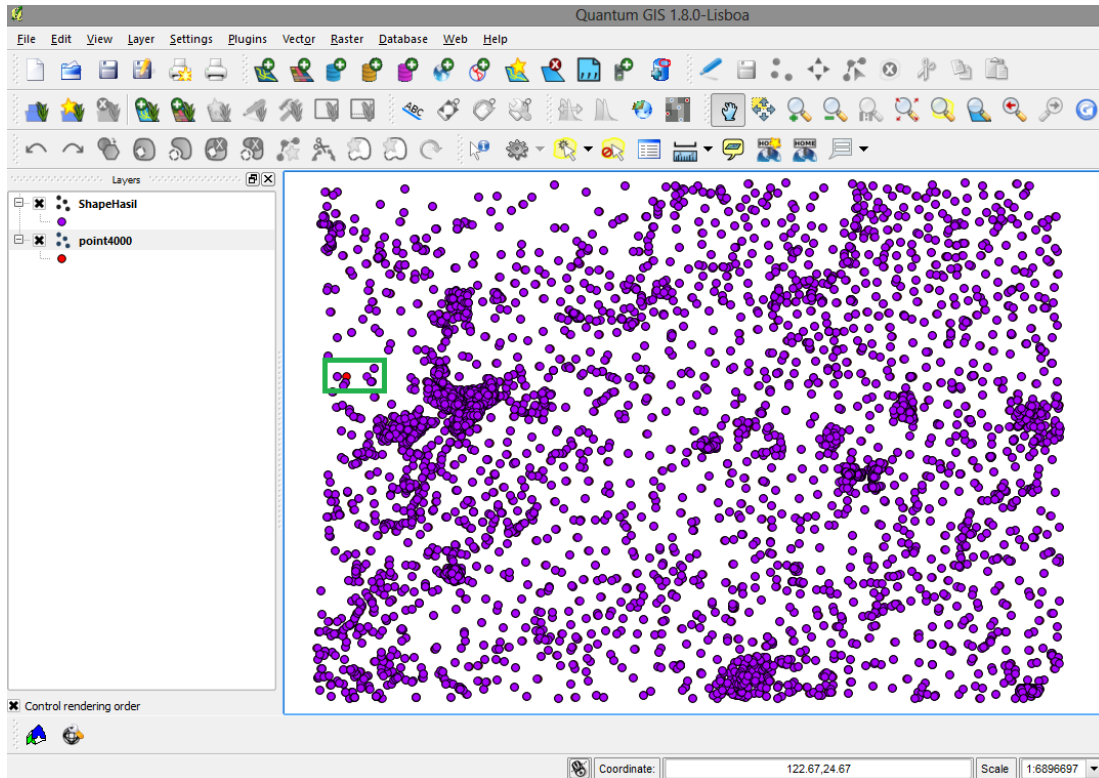

Figure 3. Original and watermarked map overlaid with each other.

Table 3. Result of fidelity test between original map with watermarked map

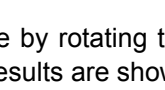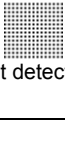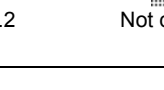| Map	Watermark	Size of Watermark (byte)	Farthest Distance (meter)
Linestring		178	0.25
		154	0.25
		174	0.26
Point		178	0.5
		154	0.5
		174	0.51
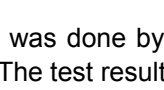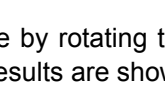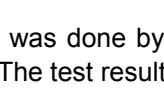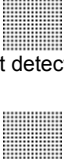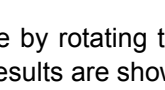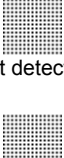
3.4. Robustness Evaluation

The testing process was then performed to determine the level of watermark robustness from the techniques developed to deal with attacks that have been prepared. Three types of geometric attacks, namely translation, rotation, and scaling attacks. Attacks were applied to the

test data in the form of vector maps that have spatial features with 4008 vertex points that have been inserted watermarks sized 178 bytes (29 x 29 pixels).Attacks carried out on test vector maps that have been inserted watermark used features provided by the software Quantum GIS. NC calculations performed on the watermark extraction results to determine the extent of the changes that occur due to these attacks. Another type of testing was also conducted to see the impact of RSA implementation as the data origin authentication toward watermark robustness level.

Translation attack wasdone by changing the position of some vertices by moving some coordinates on test data. The test results can be seen in Table 3.

Table 4. Result of translation attacks test

Amount of vertexs	Translation	Watermark Extracted (with RSA)	NC (with RSA)	Watermark Extracted (without RSA)	NC (without RSA)
1	0.1		1		1
1	0.2		1		1
1	0.3		1		1
1	0.4 k	Not detected	-		0.9939
2	0.1		1		1
2	0.2		1		1
2	0.3	Not detected	-		0.8935
(-) 2	0.1		1		1
(-) 2	0.2	Not detected	-		0.9885
3	0.1		1		1
3	0.2	Not detected	-		0.727

Rotation attack was done by rotating the entire test data coordinates in the range of -0.01 to 0.009 degrees. The test results are shown in Table 4.

Scaling attack was done by enlarging the size of the test map starting from 1.0001 to 1.0009. The test results are shown in Table 5.

Table 5. Result of rotation attacks test

Rotation (°)	Watermark Extracted (with RSA)	Watermark Extracted (without RSA)	NC (with RSA)	NC (without RSA)
-0.01	Not detected	Not detected	0	0.1035
-0.009	Not detected		0	0.3300
-0.008	Not detected		0	0.9035
-0.007			1	1
-0.006			1	1
0.006			1	1
0.007			1	1
0.008	Not detected		0	1
0.009	Not detected		0	1

Table 6. Result of scaling attacks test

Scaling	Watermark Extracted (with RSA)	Watermark Extracted (without RSA)	NC (with RSA)	NC (without RSA)
1.0005	Not detected		0	0.9980
1.0004	Not detected		0	0.9984
1.0003	Not detected		0	0.9997
1.0002	Not detected		0	1
1.0001			1	1
1.0009			1	1
1.0008			1	1
1.0007			1	1
1.0006			1	1

After implementing the three types of attacks, the techniques used did not always manage to do watermark extraction with NC value equals to one. The evaluation scenario that failed to detect the watermark was 40%. Table 4, 5, and 6 show that for the attacks that change the watermark bit, this technique will not be able to be extracted. One of the examples is the translation attack that causes a friction towards the vertex which causes the inserted watermark bit value changes and the extraction cannot be done. Beside it is seen on the rotation attack results on Table 4, the bit value change as much as 1 will make the watermark extraction fail. Therefore, the FFT algorithm will be able to maintain the real watermark value on a certain limit, but when the attack can no longer be maintained by the FFT, the watermark bit value will change and the extraction can no longer be executed.

We can say that this watermark extraction failure is caused by a quite big distortion on the watermark insertion map result. One of the factors that affects the distortion value is the limitation value usage in the watermark insertion process. This research used a -0.4 to 0.6 limitation range to determine the watermark value so it can be extracted precisely. The limitation value is affected by the usage of the modification amplitude as much as 2 or the integration that happened in the FFT calculation value.

The watermark extraction success is also affected by the usage of the RSA asymmetric cryptograph algorithm as the data origin authentication service. This is evaluated by the same implementation technique but without using RSA algorithm. The result can be seen on Table a, V, and VI, NC value increased and showed that the watermark robustness has become better and the success level for the watermark extraction is getting higher. The RSA asymmetric cryptograph algorithm usage is proven to decrease the robustness level from the technique used. This research used RSA asymmetric cryptograph algorithms to authentify the java security library. This algorithm is a very sensitive one towards encrypted data changes. When an encrypted data is having a slight change, then this data will not be able to be decrypted further. Therefore, any changes happen on the bit after the attack will cause failing watermark data extraction. This will give us choices, whether to increase the watermark robustness or to increase the data origin authentication.

Eventhough the robust level was quite low, but the technique was able to maintain the watermark for some tests that can be seen on table 4, 5, dan 6. Some extraction processes show that the result of the extracted watermark is exactly the same as the original watermark and the NC value shows 1. The robustness towards attacks happened because it caused some changes on the value of the sequence complex on the vector mapping the FFT calculation that will be spread for every FFT value. This will make the changes happened doesn't affect much and the FFT value is still in the watermark extraction value limit. The result will be different when we do the insertion on the spacey domain because the coordinate value changes will affect directly towards the inserted watermark bit value. So, the calculation spread done by the FFT which is one of the transform domain methods that can maintain the watermark better than using the spatial method.

Therefore, the robustness level of the developed technique is determined by some things such as the quality of the asymmetric key algorithm used; extraction limit used; the kinds of the frequency domain algorithm, and some other important things such as data length storage and other related programming techniques.

4. Conclusion
The conclusions of this research are:
1. *Robust watermarking* technique based on the domain transform with FFT was successfully conducted to embed a copyright marker into vector map.
2. The invisibility and fidelity level shown by this experimental results of the technique proves that the similarity and fidelity level of the watermarked vector map is kept. The distortion scale represented by the RMSE value is close to zero and the farthest distance difference is 51 cm.
3. By doing insertion in the frequency domain, any changes occur on the vector map coordinate will be spread on the other frequency domain value so it will not affect significantly to the inserted copyright. It will make the inserted copyright becomes more reliable towards any changes. The level of the *robustness* technique towards any translation attacks, rotation, and scale changing reaches 60% of the whole evaluation scenarios.
4. The usage of FFT frequency domain algorithm can maintain the precision level of the result vector map, with an acceptable distortion scale.

The usage of RSA asymmetric cryptograph key algorithm gives the data origin authentication service but it will decrease the robustness level of the inserted copyright towards any geometric attack happened.

References

[1] N Wang, C Men. Reversible fragile watermarking for locating tampered blocks in 2D vector maps. *Multimed. Tools Appl.* 2013; 67(3): 709–739.

[2] S Tao, X Dehe, L Chengming, S Jianguo. *Watermarking GIS Data for Digital Map Copyright Protection*. Proceedings of the 24th International Cartographic Conferences (ICC). 2009: 1–9.

[3] L Zheng, F You. *A Fragile Digital Watermark Used to Verify the Integrity of Vector Map*. 2009 International Conference on E-Business and Information System Security. 2009: 1–4.

[4] J Kim. Robust Vector Digital Watermarking Using Angles and a Random Table. *AISS 4*. 2010; 2(4): 79–90.

[5] J Cao, A Li, G Lv. *Study on multiple watermarking scheme for GIS vector data.* 18th International Conference on Geoinformatics. 2010; 2008: 1–6.

[6] Y Xu, Q Zhang, C Zhou. A Novel DWT-Based Watermarking for Image with The SIFT. *TELKOMNIKA Telecommun. Comput. Electron. Control.* 2013; 11(1): 191–198.

[7] HTU of F & E Gao, LTU of F & E Jia, MTU of F & E Liu. A Digital Watermarking Algorithm for Color Image Based on DWT. *TELKOMNIKA Indones. J. Electr. Eng.* 2013; 11(6): 3271–3278.

[8] C Ma, Y Zhu, M Chi, Yongyong. A Novel Selfadaptive Discrete Wavelet Transform Digital Watermarking Algorithm. *TELKOMNIKA Indones. J. Electr. Eng.* 2013; 11(11): 6281–6289.

[9] J Li, Q Cao. DSDWA: A DCTbased Spatial Domain Digital Watermarking Algorithm. *TELKOMNIKA Indones. J. Electr. Eng.* 2014; 12(1): 693–702.

[10] H Suryavanshi, A Mishra, S Kumar. Digital Image Watermarking in Wavelet Domain. *Int. J. Electr. Comput. Eng.* 2013; 3(1): 1–6.

[11] Q Liu, QLDU Liu Yantai. An Adaptive Blind Watermarking Algorithm for Color Image. *TELKOMNIKA Indones. J. Electr. Eng.* 2013; 11(1): 302–309.

[12] A Al-haj, A Mohammad, L Bata. DWT – Based Audio Watermarking. *Int. Arab J. Inf. Technol.* 2011; 8(3): 326–333.

[13] PK Dhar, J Kim. Digital Watermarking Scheme Based on Fast Fourier Transformation for Audio Copyright Protection. *Int. J. Secur. Its Appl.* 2011; 5(2): 33–48.

[14] IH Sarker, MI Khan, K Deb, MF Faruque. FFT-Based Audio Watermarking Method with a Gray Image for Copyright Protection. *Int. J. Adv. Sci. Technol.* 2012; 47: 65–76.

[15] A Tefas, A Giannoula, N Nikolaidis, I Pitas. *Enhanced Transform-Domain Correlation-Based Audio Watermarking.* Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing. 2005; 2(2): 1049–1052.

[16] VBK, I Sengupta, A Das. *Audio Watermarking Based on Quantization in Wavelet Domain.* in *Information Systems Security*. R. Sekar and A. K. Pujari, Eds. Springer Berlin Heidelberg. 2008: 235–242.

[17] C Zhu, C Yang, Q Wang. A watermarking algorithm for vector geo-spatial data based on integer wavelet transform. *ISPRS Congr.*, vol. XXXVII Par, no. Spatial Data Infrastructure. 2008: 15–18.

[18] B Liang, J Rong, C Wang. A Vector Maps Watermarking Algorithm Based On DCT Domain. *ISPRS Congr.* 2010; XXXVIII(3).

[19] C Wang, L Zhang, B Liang, H Zheng, W Du, Y Peng. *Watermarking Vector Maps Based on Minimum Encasing Rectangle.* Fourth International Conference on Intelligent Computation Technology and Automation. 2011; 2: 1243–1246.

[20] X Wang, DJ Huang, ZY Zhang. A DCT-Based Blind Watermarking Algorithm for Vector Digital Maps. *Adv. Mater. Res.* 2011; 179–180: 1053–1058.

[21] A Li, W Zhou, B Lin, Y Chen. *Copyright Protection for GIS Vector Data Production.* Proceedings of SPIE. 2008; 7143: 71432X–71432X–9.

[22] A Li, B Lin, Y Chen, G Lü. Study on copyright authentication of GIS vector data based on Zero-watermarking. *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* 2008; XXXVIII Pa: 1783–1786.

[23] L Cao, C Men, X Li. *Iterative embedding-based reversible watermarking for 2D-vector maps*. IEEE International Conference on Image Processing. 2010: 3685–3688.

[24] C Wang, Z Peng, Y Peng, L Yu. *Watermarking 2D Vector Maps on Spatial Topology Domain.* International Conference on Multimedia Information Networking and Security. 2009: 71–74.

[25] L Cao, C Men, R Ji. Nonlinear scrambling-based reversible watermarking for 2D-vector maps. *Vis. Comput.* 2012; 29(3): 231–237.

[26] A Poljicak, L Mandic, D Agic. Discrete Fourier transform–based watermarking method with an optimal implementation radius. *J. Electron. Imaging.* 2011; 20(3): 033008.

[27] M Fallahpour, D Megias. High Capacity Robust Audio Watermarking Scheme Based on FFT and Linear Regression. *Int. J. Innov. Comput. Inf. Control.* 2012; 8(4): 2477–2489.

[28] H Yan, J Li. A Blind Watermarking Approach to Protecting Geospatial Data from Piracy. *JIET Int. J. Inf. Educ. Technol.* 2011; 1(2): 94–98.

[29] N Terzija. *Robust digital image watermarking algorithms for copyright protection.* der Universität Duisburg-Essen. 2006.

[30] WW Smith. *The Fast Fourier Transform.* in *Handbook of Real-Time Fast Fourier Transforms: Algorithms to Product Testing.* Wiley-IEEE Press. 1995: 27 – 34.

[31] R Ohbuchi, H Ueda. Robust watermarking of vector digital maps. *Multimed. Expo.* 2002: 577–580.

[32] X Niu, C Shao. A survey of digital vector map watermarking. *Int. J. Innov. Comput.* 2006; 2(6): 1301–1316.