Watermarking Study on The Vector Map

[1]Hartanto Tantriawan, [2]Rinaldi Munir
[1,2]School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia
[1]Departement of Informatic Engineering, Institut Teknologi Sumatera, Indonesia
Email: [1]33220314@std.stei.itb.ac.id, [1]hartanto.tantriawan@if.itera.ac.id, [2]rinaldi.munir@itb.ac.id

Article Info
Article history:
Received Feb 20th, 2023
Revised Mar 27th, 2023
Accepted May 23th, 2023

Keyword:
DFT
DWT
Space-Domain
Transform-Domain
Watermarking

ABSTRACT
In addition to being employed in a variety of military and security applications, GIS vector maps are frequently used in social, environmental, and economic applications like navigation, business planning, infrastructure & utility allocation, and disaster management. Given the high value of this map, copyright protection is implemented in the watermarking as a required safeguard against unauthorized modification and exchange of GIS vector maps. *Watermarking* is inserting information (*watermark*) stating ownership of multimedia data. This paper discusses several approaches that can be used to watermark vector maps, including using the space-domain *algorithm* and transform-domain *algorithm.* Second The watermarking algorithm was developed with the following quality metrics: *fidelity, robustness, capacity, complexity, and security*. The challenge in this study is that the higher the capacity, the lower the fidelity value. Low fidelity causes map properties to be lost, making the map unusable. These two things need to be balanced.

Corresponding Author:
Hartanto Tantriawan,
Departement of Informatic Engineering,
Institut Teknologi Sumatera,
Gedung D212 Terusan Ryacudu Road, Way Huwi, South Lampung 35365.
Email: hartanto.tantriawan@if.itera.ac.id
DOI: http://dx.doi.org/10.24014/ijaidm.v6i1.22211

1. INTRODUCTION

Data exchange through networks is now incredibly simple because to the Internet and computer communications quick development. On the other hand, digital copyright protection for various digital media is also important. Watermarking has been studied for decades as the most popular solution to this problem. In addition to copyright protection, watermarking can also be designed for other purposes such as hiding communications, data authentication, and data tracking.

In general, location data, attribution data, and some other data used as an index or description make up vector map data. Spatial data always takes the form of the three fundamental geometric shapes of points, polylines, and polygons and represents the location of map objects that reflect geographic things in the real world. Each of these map objects is made up of several carefully placed vertices. A list of these vertices' coordinates in a particular geographic coordinate system is called spatial data. Map object attributes like name, category, and other details are described through attribution data. No other data may be added to or subtracted from the crucial information captured by attribution data. The geographical data, specifically the node coordinates, offer the space for embedding the watermark in each of the suggested watermarking techniques [1].

Several studies have been developed taking into account Fidelity, Transparency, Imperceptibility [2], payload watermark robustness and security factors [3], Reversibility [4], false positives [5][6], and topology [7]. Many studies have also been created employing two algorithmic domains, namely the space-domain and the transform-domain, in addition to paying attention to these elements. By directly changing the coordinate values of the nodes in the space-domain, watermarks are embedded utilizing a variety of techniques, including node locational relations, coordinate statistical features, etc. Whereas in the transform domain of vector map watermarking, the data watermark is incorporated in the transformation coefficient rather than the node coordinates directly. DFT, DWT, and DCT are the transformation schemes that are employed [8].

Keypoint-based watermarking is used by Cao[9] to stop unauthorized users from gaining unlawful access to vector geographic data. The three feature layers that are taken into consideration are the point, linear, and areal feature layers. The keypoint coordinates for each feature layer are chosen to serve as the watermark. Following that, the watermark is encrypted and added to the LSB keypoint coordinates (Least Significant Bits). Similar techniques are used to find watermarks, such as extracting the embedded watermark from the LSB keypoint coordinates. Large distortion and poor watermark capacity in lossless watermarking are two issues that frequently occur in present watermarking systems for 2-D vector maps. A recursive embedding approach was proposed by [9] as a solution to these issues. Each polyline's feature points are retrieved and grouped. The watermark is iteratively inserted into the highly correlated data set that was selected as the watermark embedding point by modifying the coordinates of the median vertex of each insertion unit. The steps for watermark extraction and data recovery are similar. High capacity and fidelity are attained by their plan[9].

Reversible data-hiding methods were improved by Wang et al. [10]. This is achieved through a data-hiding technique based on virtual coordinates. The distance between the highest and least coordinates of each coordinate is divided into several components. In order to build an interval that can carry the watermark by modifying its state value, two virtual coordinates are created for each point in the segment.

In their paper, Peng et al. offer a blind watermarking technique for polyline features in vector maps. The location of the watermark embedding is determined by building the feature vertex distance ratio for polyline features with a slight modification using quantization index modulation. This technique is resistant to object, vertex, and geometric attacks [11].

A reversible watermarking system based on normalized nodes is described by Nana Wang. The 2-D vector map's vertices are translated into new coordinates. The normalized node is determined for each node using IQIM and is then utilized as the embedding position for the watermark. This method is resistant to straightforward geometrical attacks [12]. The watermarking method suggested by Yan et al. involves normalizing each vertex on a vector map. After that, the watermark is duplicated and repeatedly inserted in the normalized map nodes. During the watermark extraction phase, this approach is resistant against geometric and vertex attacks but is vulnerable to rotation [13]. It also does not require the original map.

Qiu et al., introduces a brand-new high-loading reversible watermarking method for vector maps. The QR (Quick Response) code is used as a watermark in the system and is included in the vector map's Polar Coordinates. It can tolerate noise attack and some degree of knot alteration [14].

Watermarks are incorporated into the vector map elements that cause distortion in order to confirm the authenticity and integrity of 2-D vector maps. In terms of information security, this is intolerable. Wang [15] employs a reversible watermarking approach to avoid distortion.

The spatial characteristics of 2-D vector maps were categorized into a variety of classes by Wang et al. based on various record counts. During the watermark verification phase, each feature location is marked in order to identify the original feature of each group. This method precisely recovers the original content in addition to identifying and locating altered groups. The following are the scheme's drawbacks: I Only polyline characteristics are used in this scheme. (ii) Only altered feature groups are detectable by this method. Nana Wang and Chaoguang Men suggested a reversible fragile watermarking strategy in order to identify and locate tampered blocks in the vector map and to guarantee the restoration of the original contents. There are simple blocks and regular blocks in the vector map feature. Wang and Wang improved the reversible watermarking approach and used it to validate regular blocks. Meanwhile, a flimsy vertex insertion-based watermarking approach is used to authenticate complicated blocks. Their systems are capable of identifying and detecting malicious activities such node addition, removal, and modification [16].

Nana Wang and Mohan Kankanhalli have introduced a novel fragile watermarking approach that can be used to pinpoint the original location of the altered features. Features on vector maps are separated into different categories. In each group, the embedded watermark is created using the location bit and check bit. To identify the altered group and identify its current region, the extracted and computed check bits are compared. This scheme's disadvantage is that it is impossible to identify the original location of the damaged group when the broad area vector map has been altered [17].

2. RESEARCH METHOD

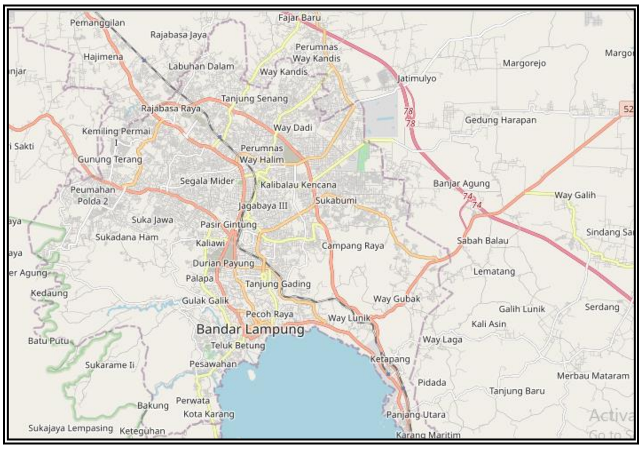
2.1. Vector map data structure

The usage of a geographic information system (GIS), a computer-based system, facilitates the entry, storage, manipulation, and output of location-based geographic data. The two subcategories of GIS data models are raster and vector. Satellite images are the most well-known application of a raster model in GIS.

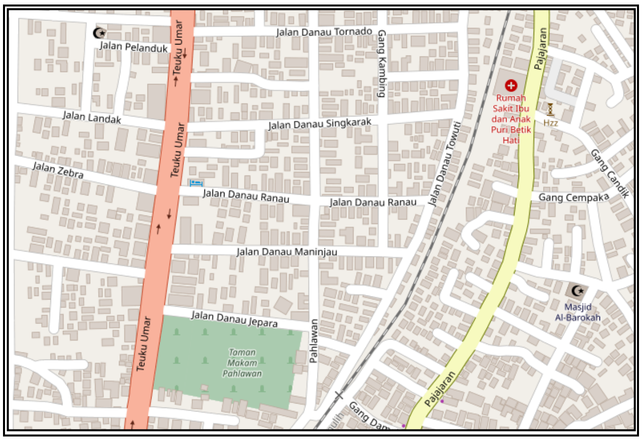
This study focuses on three GIS vector data elements: spatial data, attribute data, and index data. Three basic geometric objects are always used to describe spatial information, which explains the map itself [18]:

1. Point - used to represent physical items like bus stops, traffic lights, and streetlights, points specify a specific location for an object.
2. Polylines - linear objects are defined by line entities, which might be as straightforward as a two-point line or as intricate as a thread with several knots. Actual objects like rivers and motorways are depicted by lines.
3. Polygon - area-based objects are created using polygon entities, which might be square or have numerous vertices and sides. Lakes, shopping centers, structures, and city limits are all represented by polygons.

The three basic entities of this vector map can be seen in Figure 1 [19].



(a)



(b)

Figure 1. Map of Bandar Lampung City

Figure 1(b) shows Points - point entities described by 'Puri Betik Hati Hospital' and 'Al-Barokah Mosque' is an x,y coordinate point. Polylines - line entities defined by several street names such as 'Jalan Danau Jepara', 'Jalan Danau Maninjau', 'Jalan Danau Ranau', and several other roads. Polylines are a series of ordered x and y coordinates. Polygon - a polygon entity represented/described by the complex 'Garmet of Heroes(Taman Makam Pahlawan)' a series of x,y coordinates covering an area.

Via connections to location data, attribute data describes mapping entity properties. Matching names or addresses are just two examples of attributes. The most well-known example of a GIS attribute data format is an ESRI database file that is linked to an ESRI form file and has the same prefix as the form file [19].

The structure of a file, such as the overall file length, is described by index data in the context of a GIS, whether it be for attribute or geographic data. The most well-known illustration of index files is provided by ESRI's [19] index files. Vector data formats that can be distinguished from picture data present additional difficulties for researchers studying digital watermarking.

2.2. General Watermarking System

A watermark, an encoder (insertion method), and a decoder are the three main parts of a watermarking technique (extraction algorithm). The three stages of the watermarking process are the Encoding Process, the Decoding Process, and the Comparing Process. The technique of integrating a watermark into a multimedia object is called encoding. Figure 2 shows this procedure.

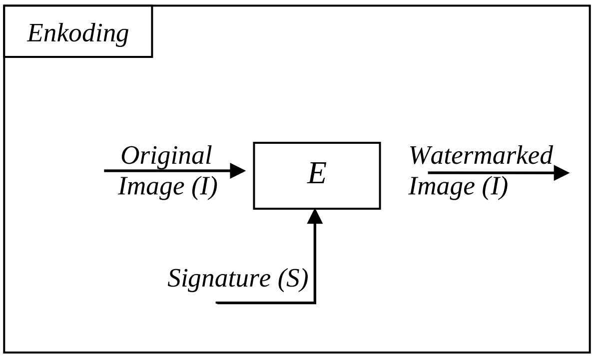


Figure 2. Encoding process

The encoding process can be denoted into a mathematical equation in equation 1 below [25],

$$E\,(\,I,S\,) = \hat{I} \tag{1}$$

Where I is Image, and S is Signature (watermark). E is the insertion function which will combine the Original Image and Signature to become Î, a new image that has been given a watermark (watermarked image). The decoding procedure is the following step. A decoder function D will accept an input image J. (J can be an image that has been given or has not been given a watermark). Function D will return the value S' (signature of image J). This process can be seen in equation 2.

$$D\,(\,J, I\,) = S' \tag{2}$$

I, a version of J that isn't watermarked, can also be added throughout this process. The addition of image I is done to produce better robustness as well because there is a potential for damage to a pixel in the decoding process. Figure 3 depicts this process [20].

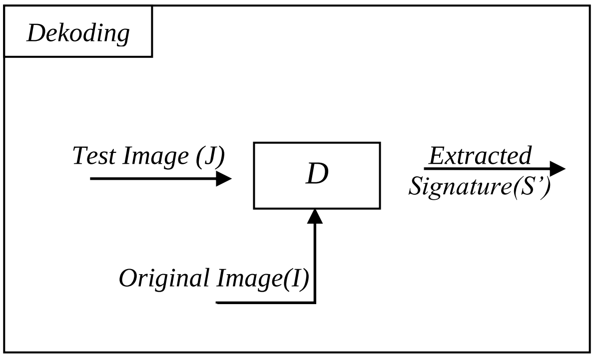


Figure 3. Decoding process

The function C_δ will be used to compare the extraction signature S'. Which output as a binary number. Function C_δ will be worth 1 if the result of the extraction comparison signature is equal to the signature beginning. Instead, it will be worth 0 if the results of the comparison signature it doesn't match. This can be written according to equation 3 below:

$$C_\delta(S,S') = \begin{cases} 1, c \leq \delta \\ 0, otherwise \end{cases} \tag{3}$$

Where C is a correlator, $x = C_{\delta}(S, S')$. c is the correlation between the two signatures, and δ is the threshold [20]. The relationship between the decoding and comparison functions can be seen in Figure 4 below.

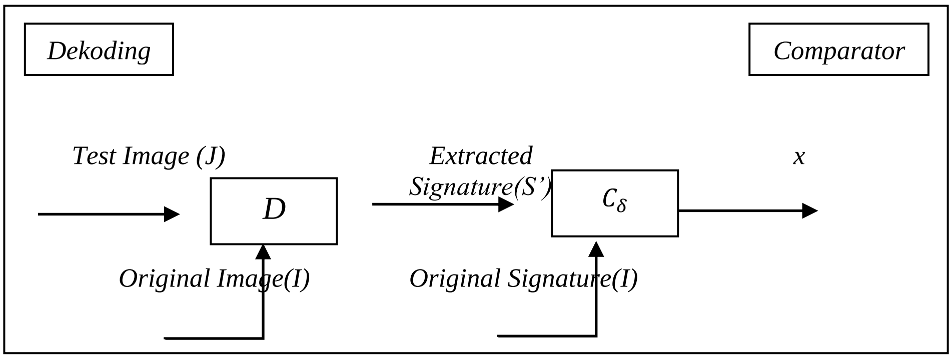


Figure 4. Decoding and Comparator Process

2.3. Watermarking on vector maps

GIS vector maps are widely used in environmental, social, and economic applications such as disaster management, navigation, distributing infrastructure and utilities, and planning for businesses. They are also utilized for military and security purposes. These maps are valuable, and as a result, they must be protected to prevent unethical usage in situations involving both national and global security, as well as to stop attackers from gaining a capital gain.

Several copyright strategies, the majority of which fall into the two categories of encryption and information concealing, have been utilized to prevent the unauthorized modification and exchange of vector GIS maps. A cryptographic system that tries to safeguard a message's or file's contents includes encryption. Many disciplines use information concealment, but steganography and watermarking are the most prevalent. Whereas the goal of watermarking is to prevent concealed information from being seen, the goal of steganography is to retain the secrecy around the existence of the information [21]. The most often used method of copyrighting vector GIS maps is approach watermarking.

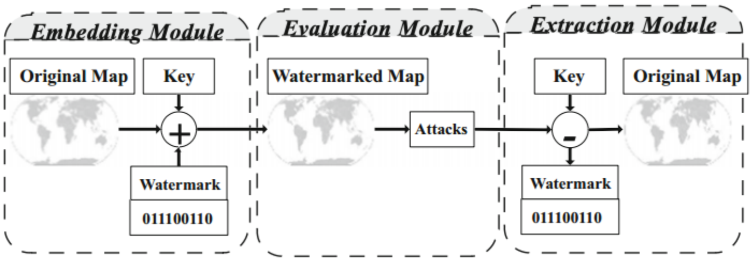


Figure 5. General system watermarking digital vector map

The approach for watermarking maps is made up of three components: embedding, evaluation, and extraction, as shown in Figure 5 [18]. The embedding module uses a secret key to partially conceal watermarks inside the original map material (required in the extraction stage). Using specific assessment metrics, the evaluation module will evaluate the approach watermarking map's quality. Making a claim regarding data ownership is crucial, and the extraction module uses an extraction watermark. In research watermarking, GIS maps with raster data formats have gotten more attention than digital GIS vector maps [22].

2.4. Digital copyright protection algorithm

The three basic modules that make up the digital map copyright protection system are embedding, evaluation, and extraction.. An overview of some of the algorithms used for the approximation watermarking is given in Table I.

Tabel 1. Watermarking algorithm

Term	Definition	Reference
Zero watermarking	Aims to produce watermark data by using some of the data host's essential characters.	[23]

Term	Definition	Reference
Adaptive watermarking	Attempts to create a watermark based on some regional features of the original data.	[24]
Multiple watermarking	Refers to the insertion of several watermarks into host data.	[25]
Reversible / Lossless watermarking	Seeks to recover the original data after the extraction watermark and attempts to strike a fair balance between the embedding process and data quality watermark.	[9]
Classic watermarking	Refers to the area in which the watermarking method is used on various image data types.	[26]

2.5. Watermark Embedding Module

Digital watermarks may be embedded into either the space domain or the transform domain, depending on the embedding domain. By changing the node coordinate values, the watermark is directly implanted in the space-domain. In the transform domain, data watermarks are embedded by altering their transformation coefficients rather than the vertices' physical coordinates.

To pin watermarks based on various embedding schemes and to shift map vertices within predetermined tolerances, space-domain approach watermarking is used.

Figure 6 shows several different ways to represent the embedding space domain: blocks, topological relationships, polar coordinates, and Cartesian coordinates.

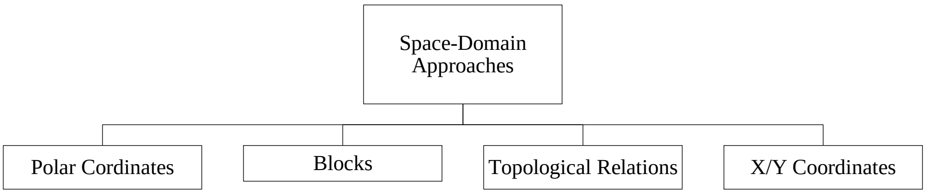


Figure 6. Classification of techniques in the space domain.

To protect GIS data quality from rotation attacks and translation, the embedding topological relations approach refers to the input watermark process into the map topology rather than node coordinate values (such as distances between map vertices) [27]; the embedding cartesian coordinates approach uses direct vertex coordinate values to enter the watermark [28].

The vector map is divided into parts (blocks) via the embedding block-based technique, which aids in improving resilience to noise attack and simplification[20]. This method can maintain integrity to a certain extent and reasonably locate watermark remnants in specific blocks [29].

The embedding polar coordinates method involves directly embedding the watermark using a different kind of node coordinate value. This strategy achieves robustness similar to the Cartesian coordinate-based strategy, which is advantageous for attacks like translation, the same rotation, and scale [30].

Space-domain The simplicity, low computing complexity, and potential of large capacity of the proposed scheme are its benefits (i.e., size watermark). The space-domain scheme's fundamental drawback is its limited resilience, making it susceptible to several assaults.

In contrast to the space domain, the schematic embedding transform domain embeds a watermark by changing the transformation coefficients of the vertices rather than their coordinates. Figure 7 illustrates the most common types of transformation: cosine transformation, wavelet transformation, and transformation fourier (CT).

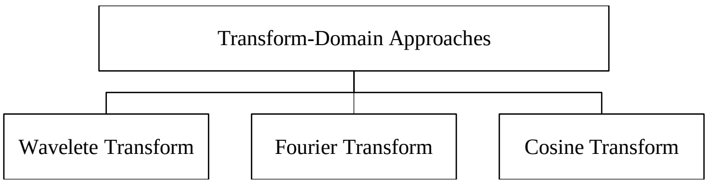


Figure 7. Classification of techniques in the transform domain

Digital vector maps are segmented into several categories and layers using a sort of analysis called WT. In the face of noise, rotation, and scaling, the wavelet-based approach is resilient[31]. To meet the ideal balance between robustness and invisibility, FT is a digital transformation that gives the option to modify the frequency of the host-vector map. This aids in choosing suitable spots for bits watermark embedding into vector maps. The primary benefit of FT is that it is invariant to some geometrical attacks, including translation, scaling, and rotation[32]. Another digital transformation called CT divides the vector map into portions with varying frequencies according to the vector map's visual quality. The fundamental property of CT is a large energy concentration at minimal coefficients with reduced overall computational costs[33].

The most widely used algorithm for the embedding method in the transform-domain is:

1. Watermarking using Wang's (DFT-Based) technique.
2. Sangita's (DWT-Based) watermarking technique.

2.5.1. Watermarking using Wang's (DFT-Based) technique.

Since DFT-DF based watermarking has the distinct advantage of being resistant to geometric attacks, it is a widely utilized technique. [34]. The embedding watermark process denoted as follows $W = \{w_m = 0,1 | m = 0,1,\ldots, N-1\}$ N stands for the watermark sequence's length. The value is 0 for the watermark extraction process at w_m must be converted with a value of -1. Once converted, $W = \{w_m = \pm 1 | m = 0,1,\ldots, N-1\}$. Equation (4) converts the initial vertex sequence $\{v_k = (x_k, y_k)\}$ into a vector map and a complex sequence:

$$a_k = x_k + i * y_k \tag{4}$$

Where the vertex k horizontal and vertical coordinates are x_k and y_k, respectively. A complicated sequence is a_k. Use equation (5) to calculate the discrete fourier transform (DFT) process on ak to obtain the DFT coefficient:

$$A_l = \frac{1}{N} \sum_{k=0}^{N-1} a_k \left(e^{-2\pi j}/_N\right)^{kl}, l \in [0, N-1] \tag{5}$$

DFT coefficients of the sequences A_l consists of amplitude $\{|A_l|\}$ and phase $\{|\angle A_l|\}$. The information about the watermark is then added to the phase sequence in accordance with the embedding rule. Equation (6) below shows how the embedding watermark algorithm is represented:

$$\angle A'_l = A_l + \rho * w_m \tag{6}$$

Which ρ represent to embedding power. IDFT (Inverse discrete fourier transformation) process to get watermark complex sequence $a'_k = x'_k + i * y'_k$ did by combining watermark phase $\angle' A_l$ with amplitude $|A_l|$. Watermarked vector map G' can be obtained by set the ordinate value at the node, according to a'_k. Watermark extraction is inverse of the insertion process (embedding) watermark. The ordinate value of the node on watermarked vector map G' look for collected by using $a'_k = x'_k + i * y'_k$. Sequence a'_k represent a combination of phase watermarks $\angle' A_l$ with amplitude $|A_l|$. The value $\angle A'_l$ can be obtained using equation 6. Then the amplitude $|A_l|$ can be calculated using equation 5. After the amplitude was obtained, so the sequences a_k calculated using equation 4. The next a_k converted to w_m. DFT-based watermarking process flow chart is shown in Figure 8.

2.5.2. Sangita's (DWT-Based) watermarking technique.

High-frequency coefficients can be regarded as noise in DWT-based watermarking [35]. In vector maps, the high-frequency coefficients frequently undergo significant change whereas the low-frequency coefficients exhibit greater stability. As a result, the watermark information embedded in the DWT low-frequency coefficient will have strong noise resistance. Two layers of a discrete wavelet transform are applied to the original vertex sequence $\{v_k = (x_k, y_k)\}$. The insertion algorithm is notated in equation (7):

$$L(x)' = L(x) + \rho * w_m \tag{7}$$

In order to create a vector map with a watermark, the watermarked low-frequency component, L(x)', underwent inverse discrete wavelet transformation (IDWT) with three additional coefficients. The two most significant coefficients are displayed in the flow chart in figure 9. The strategy for the transformation domain is robust against geometric assaults like rotation, translation, and scaling, but it has the drawback of being challenging to put into practice and having a high level of computational complexity. Process-induced vertex disturbances incorporating a watermark may have an impact on topological and geometric properties. A post-correction method on topology and geometric aspects on two-dimensional vector maps is suggested by Xu Xi's research [36]. Figure 10 details the data rectification and watermarking procedure.

Figure 10 describes that the input data is a vector map which is denoted as G. watermark information is denoted by w_m. the output is a vector map that has been watermarked with a notation *G'* Which which has the same topology and geometric features as G [36]. Step 1: Using the initial vector map G, determine the MPR (maximum perturbation regions) of each node (vertex). Step 2: Insert watermark data into the G' generates a watermarked vector map using two separate watermarking methods. Check the watermarked node for dirt in step three. A watermarked node's topology and geometric properties are well-preserved if it is found in the MPR. Otherwise, filthy nodes with possible topology flaws or missing geometric features must be found and fixed. Checking whether a node is breaking topological or orientation restrictions is the key component of dirty node detection. When inserting a watermark, one of these constraints, the topological constraint, requires determining whether the line intersects itself or other elements. The direction constraint, on the other hand, requires determining whether the change in the direction angle of the point connection line exceeds a certain threshold. A Filthy Knot Correction is stage four. The coordinate adjustment method based on the topological association of the same node will be used for dirty knots AND' in order to improve it. The topology and geometric shapes of the vertices are well preserved after correction, if AND' within the MPR. To satisfy the topological and orientation restrictions, the vertices will be forced shifted to the MPR if they are still outside of it. Stage 5. Rerun Stage 3, this time looking for nearby vertices of the fixed vertices. Step 4 can be used to fix any dirty nodes that are still present. Till all nodes adhere to the topology and direction requirements, repeat the previous procedures. Step 6: The watermarked vector map G' is eventually produced.

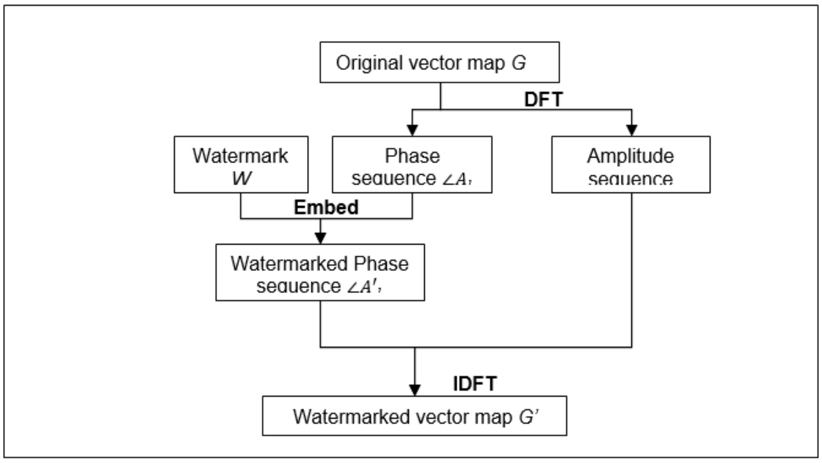


Figure 8. DFT-based watermark embedding flowchart

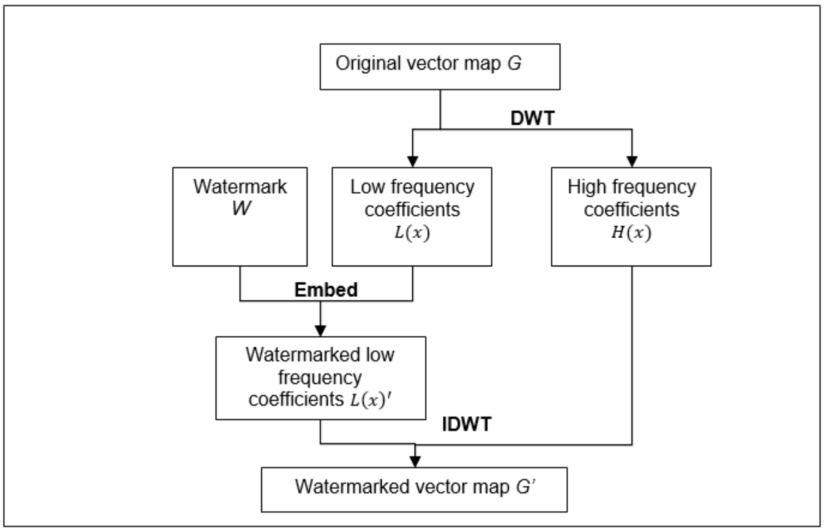


Figure 9. DWT-based watermark insertion flowchart

An example of vector map experimental data can be seen in Figure 11. The Shenzhen city vector map has 1145 polygons. The process of embedding watermarks will alter the coordinates and induce deviations in the vector map's elements, resulting in the creation of 16,247 vertices[36].

Figure 11. Vector map of the city of Shenzhen.

The watermark used is a binary image with dimensions of 80x80 and 32x32 containing copyright messages 'SYSU ZERO'. Watermark is attached to picture 12. In Figure 13, the original map and the watermarked vector map are superimposed. On a vector map that has been watermarked, points are displaced.

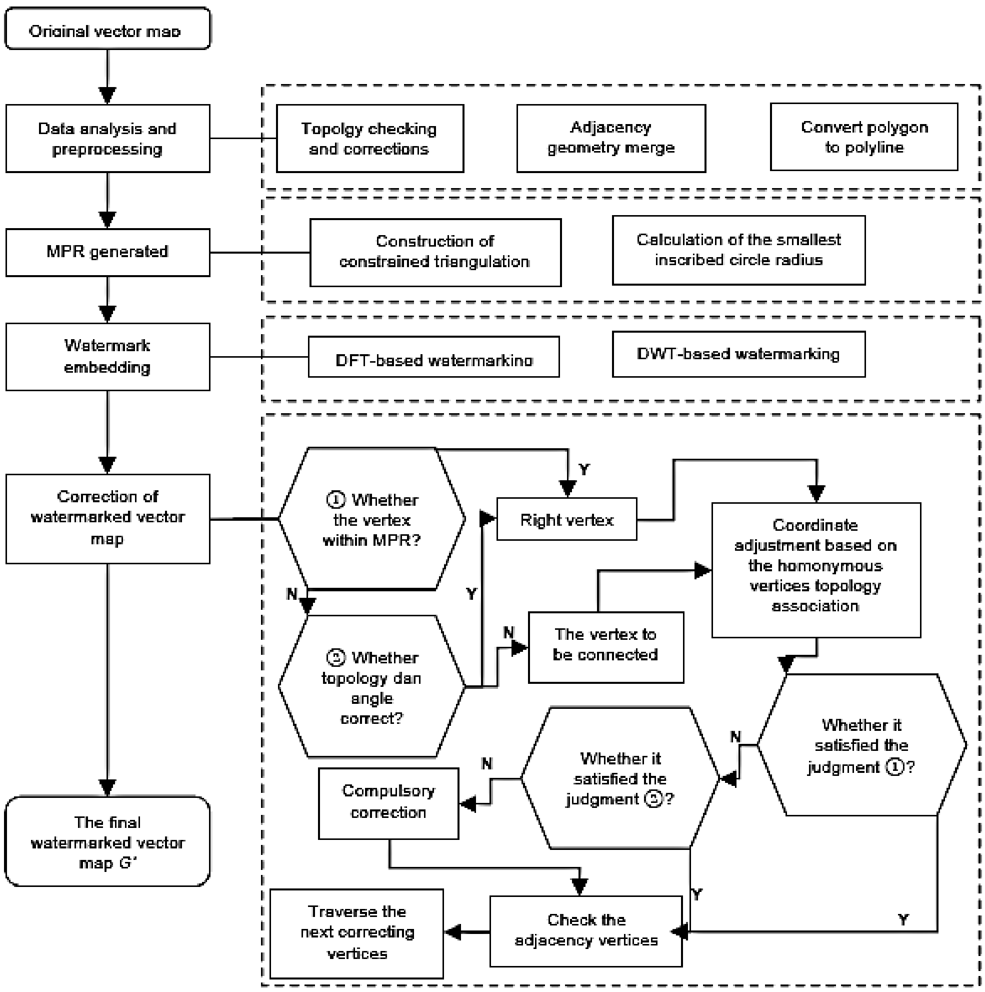


Figure 10. The watermarking method with topology and geometric features.

Figure 14 demonstrates that the SZ city map clearly exhibits a geometric loss following the addition of the watermark. Figures 14b and 14c exhibit data for updated watermarks and corner deformation in SZ. The outcomes demonstrate that, following the embedding of watermarks, the correction procedure is successful in maintaining the topological and geometric properties [36]. Table II provides a summary of the watermarking technique.

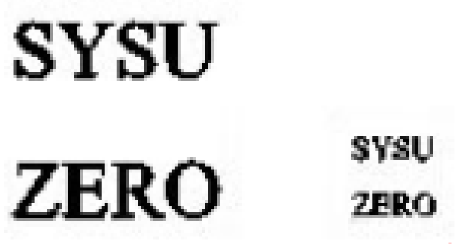


Figure 12. Watermark Images

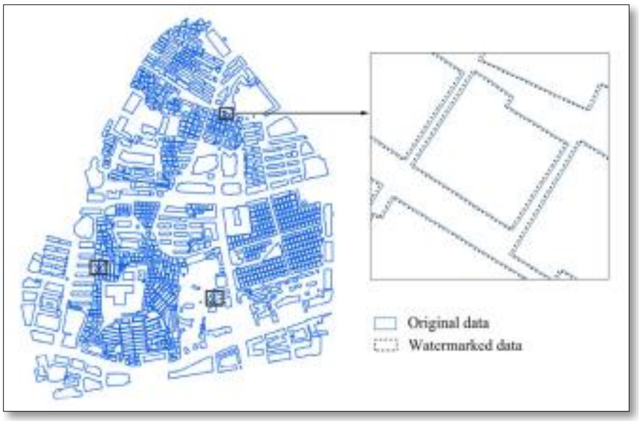


Figure 13. Overlay vector map original and watermarked

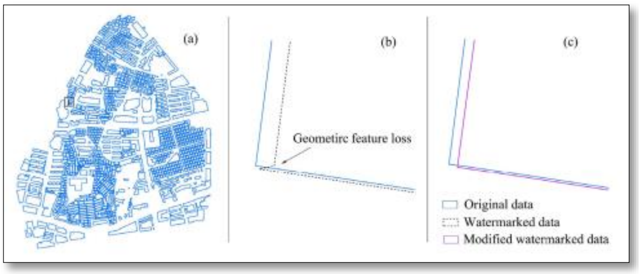


Figure 14. Embedding of watermarking and the results of DWT-based watermarking corrections in SZ. (b), (c) occurs at the place marked 1 in (a)

2.6. Watermarking Evaluation Module

The evaluation module evaluates the approach's watermarking quality by evaluating a number of factors, including: (a) the map's quality after the watermark is inserted (fidelity); (b) the map's resistance to attack (resistance/robustness); (c) the coverage watermark (capacity); (d) the approach's computational complexity (complexity); and (e) the site security watermark in the map (security) [18]. Measurement of watermark similarity as shown in Figure 14 can be done by one of them by NC (Normalization Correlation). NC can be calculated using the following equation 8:

$$NC = \frac{\sum_{ij} W_{ij} * W'_{ij}}{\sqrt{\sum_{ij} W_{ij}^2}\sqrt{\sum_{ij} W'^2_{ij}}} \quad (8)$$

NC is a useful technique for analyzing the similarity between the initial coordinates and the extracted coordinates. The value of this technique ranges from 0 to 1. The fact that this procedure produces a greater NC value suggests that the reversible watermarking outcome will be similar to the first or won't differ significantly from it. The NC calculation uses Equation 8 with In as the bit watermark early and In' is the result bit watermark extracted [36].

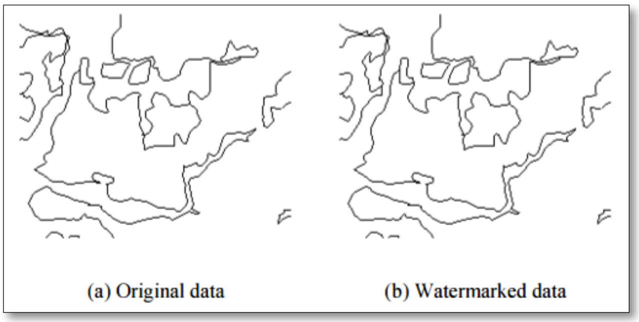


Figure 14. An example of an original vector map (a) and a watermarked map (b) [37]

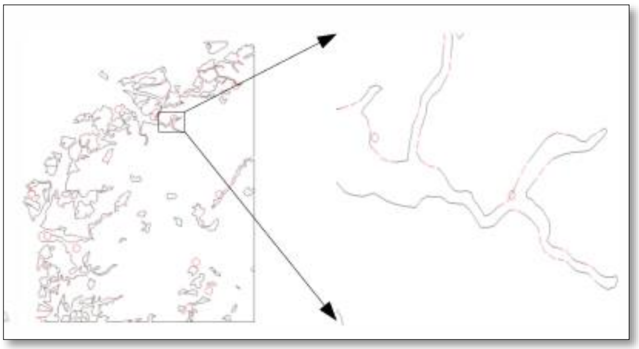


Figure 15. Noise due to watermarks [37]

Error / Noise on the data (Figure 15) can be measured in several ways. Some of them are RMSE, PSNR, and MSE. The error between the data (coordinates) after watermarking and the unwatermarked data (coordinates) is measured using RMSE. Equation 9 can be utilized to determine RMSE.

$$RMSE = \sqrt{\frac{1}{N} \sum_{i=1}^{N_v} (x'_i - x_i)2 + (y'_i - y_i)} \quad (9)$$

PSNR is a mathematical approach from human perception to the quality of data reconstruction. PSNR is obtained using equation 10.

$$PSNR = 10 \log 10 \left(\frac{Max_I^2}{MSE}\right) \quad (10)$$

The maximum value of a pixel in a picture is called Max I. The maximum value is 255 if an 8-bit picture is being used.

3. DISCUSSION

The watermark is concealed within the original map as part of the embedding module. Either space-domain or transform-domain approaches can be used for embedding. The simplicity, low computational complexity, and prospective expansion of the watermark capacity are the benefits of the space-domain technique. The space-domain scheme's fundamental drawback, however, is its susceptibility to some assaults and hence limited robustness. The transform-domain approach has the drawback of being challenging to construct even though it is robust against geometric attacks like rotation, translation, and scaling. This approach also has a high level of computational complexity. It is challenging to experiment with different amounts of capacity in the transform-domain scheme and see how it affects other features like fidelity and resilience since the capacity aspect is more difficult to regulate than it is in the space-domain scheme.

There is still room for improvement in a number of embedding module-related areas, including (a) what attacks are pertinent for vector data to match watermark maps' robustness? (b) the capacity fidelity trade-off, including the ramifications for embedding location selection. Because they have an impact on the site of embedding, they are strongly tied to evaluation modules.

Various attacks can alter a watermarked map by altering the watermark (which would make it impossible to determine who the true owner is) or the map itself. Attacks can be divided into two major categories: geometric and signal operation attacks. It has been demonstrated that geometric transformations (such as rotation and translation) can be easily undone on vector data with little data loss. Hence, signal operation attacks should be the main target (eg simplification, addition of noise, interpolation).

Two crucial variables for assessing a watermarking strategy are capacity and fidelity. As a result, capacity and robustness are coupled. In contrast, fidelity refers to the quality of the map after the watermark has been added. Because the larger the capacity, the more the noise that is added into the map, which results in lower fidelity, these two measures must be balanced. Poor fidelity indicates the watermarked map cannot be used since some map attributes are lost, especially those relating to point/node fidelity. One of the features of vector data that makes them so valuable is fidelity, particularly for situations where fidelity is crucial, like military operations. Hence, in studies on watermarking vector map data, the balance between these two measures becomes crucial.

4. CONCLUSION

GIS vector maps are often used in environment, economic, and socioeconomic applications such as disaster preparedness, navigation, distributing utility services and infrastructure, and management for businesses. They are also utilized for military and security purposes. Because of the usefulness of these maps, copyright protection is essential to prevent both immoral usage in circumstances involving national and international security as well as adversaries getting an economic advantage. Several copyright strategies have been employed to prohibit the unauthorized modification and exchange of vector GIS maps; the watermarking method is the most often used method.

The watermarking algorithm used on vector maps must be effective when measured by the following criteria: (a) the quality of the map after the watermark is inserted (fidelity); (b) the robustness of the watermark map against attack; (c) watermark coverage (capacity); (d) the computational complexity of the approach (complexity); and (e) the security of the location of the watermark on the map (security).

Based on the literature review that has been described, therefore research that has the potential to be developed is watermarking on vector maps using a transformation approach with good imperceptibility and resilience as well as high capacity.

ACKNOWLEDGEMENTS

This work was supported by Institut Teknologi Sumatera [T/436/IT9.A/KP.06.00/2021].

REFERENCES

[1] B. Lin and A. Li, "Study on benchmark system for copyright marking algorithms of GIS vector data," 2010. doi: 10.1109/GEOINFORMATICS.2010.5567749.

[2] S. Huber, R. Kwitt, P. Meerwald, M. Held, and A. Uhl, "Watermarking of 2D vector graphics with distortion constraint," 2010. doi: 10.1109/ICME.2010.5583049.

[3] C. Wang, L. Zhang, B. Liang, H. Zheng, W. Du, and Y. Peng, "Watermarking vector maps based on minimum encasing rectangle," in *Proceedings - 4th International Conference on Intelligent Computation Technology and Automation, ICICTA 2011*, 2011, vol. 2. doi: 10.1109/ICICTA.2011.589.

[4] F. L. Bauer, *Decrypted secrets: Methods and maxims of cryptology*. 2007. doi: 10.1007/978-3-540-48121-8.

[5] "Information hiding terminology," 1996. doi: 10.1007/3-540-61996-8_52.

[6] D. Kahn, "The history of steganography," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1996, vol. 1174. doi: 10.1007/3-540-61996-8_27.

[7] H. Berghel, "Watermarking cyberspace," *Communications of the ACM*, vol. 40, no. 11, 1997, doi: 10.1145/265684.265687.

[8] F. Perez-Gonzalez and J. R. Hernandez, "Tutorial on digital watermarking," 1999. doi: 10.1109/ccst.1999.797926.

[9] L. Cao, C. Men, and Y. Gao, "A recursive embedding algorithm towards lossless 2D vector map watermarking," *Digital Signal Processing: A Review Journal*, vol. 23, no. 3, 2013, doi: 10.1016/j.dsp.2012.11.007.

[10] N. Wang, H. Zhang, and C. Men, "A high capacity reversible data hiding method for 2D vector maps based on virtual coordinates," *CAD Computer Aided Design*, vol. 47, 2014, doi: 10.1016/j.cad.2013.10.005.
[11] Z. Peng, M. Yue, X. Wu, and Y. Peng, "Blind watermarking scheme for polylines in vector geo-spatial data," *Multimedia Tools and Applications*, vol. 74, no. 24, 2015, doi: 10.1007/s11042-014-2259-9.
[12] N. Wang, "Reversible watermarking for 2D vector maps based on normalized vertices," *Multimedia Tools and Applications*, vol. 76, no. 20, 2017, doi: 10.1007/s11042-016-3970-5.
[13] H. Yan, L. Zhang, and W. Yang, "A normalization-based watermarking scheme for 2D vector map data," *Earth Science Informatics*, vol. 10, no. 4, 2017, doi: 10.1007/s12145-017-0310-x.
[14] Y. Qiu, H. Gu, and J. Sun, "High-payload reversible watermarking scheme of vector maps," *Multimedia Tools and Applications*, vol. 77, no. 5, 2018, doi: 10.1007/s11042-017-4546-8.
[15] N. Wang and C. Men, "Reversible fragile watermarking for 2-D vector map authentication with localization," *CAD Computer Aided Design*, vol. 44, no. 4, 2012, doi: 10.1016/j.cad.2011.11.001.
[16] N. Wang and C. Men, "Reversible fragile watermarking for locating tampered blocks in 2D vector maps," *Multimedia Tools and Applications*, vol. 67, no. 3, 2013, doi: 10.1007/s11042-012-1333-4.
[17] N. Wang and M. Kankanhalli, "2D vector map fragile watermarking with region location," *ACM Transactions on Spatial Algorithms and Systems*, vol. 4, no. 4, 2018, doi: 10.1145/3239163.
[18] A. Abubahia and M. Cocea, "Advancements in GIS map copyright protection schemes - a critical review," *Multimedia Tools and Applications*, vol. 76, no. 10, 2017, doi: 10.1007/s11042-016-3441-z.
[19] ESRI, "ESRI Shapefile Technical Description," *Computational Statistics*, vol. 16, no. July, 1998, doi: 10.1016/0167-9473(93)90138-J.
[20] Saraju P. Mohanty, "Digital Watermarking: A Tutorial Review," 2003, Accessed: Jan. 25, 2021. [Online]. Available: https://www.researchgate.net/publication/2568630_Digital_Watermarking_A_Tutorial_Review/stats
[21] C. López, "Watermarking of digital geospatial datasets: A review of technical, legal and copyright issues," *International Journal of Geographical Information Science*, vol. 16, no. 6, 2002, doi: 10.1080/13658810210129148.
[22] T. Abbas and M. Jawad, "Digital vector map watermarking: applications, techniques and attacks ," *Oriental. J Comput Sci Technol*, vol. 6, no. 3, pp. 333–339, 2013.
[23] A. Abubahia and M. Cocea, "Partition Clustering for GIS Map Data Protection," in *Proceedings - International Conference on Tools with Artificial Intelligence, ICTAI*, 2014, vol. 2014-December. doi: 10.1109/ICTAI.2014.128.
[24] H. Peng, G. Jianya, and C. Liang, "An improved adaptive watermarking algorithm for vector digital maps," 2006. doi: 10.1109/IGARSS.2006.731.
[25] P. Bhanuchandar, M. S. G. Prasad, and K. P. Srinivas, "A SURVEY ON VARIOUS WATERMARKING METHODS FOR GIS VECTOR DATA," *International Journal Computer & Electronics Research*, vol. 2, no. 3, Jun. 2013.
[26] H. H. Chang, T. Chen, and K. S. Kan, "Watermarking 2D/3D graphics for copyright protection," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2003, vol. 4. doi: 10.1109/icassp.2003.1202744.
[27] W. Xun, H. Ding-Jun, and Z. Zhi-Yong, "A robust zero-watermarking algorithm for 2D vector digital maps," in *Lecture Notes in Electrical Engineering*, 2012, vol. 107 LNEE. doi: 10.1007/978-94-007-1839-5_56.
[28] Q. Zhao, L. Sui, C. Wang, and X. Yin, "Publicly verify the integrity of the geographical data using public watermarking scheme," in *Communications in Computer and Information Science*, 2013, vol. 398 PART I. doi: 10.1007/978-3-642-45025-9_63.
[29] L. Zheng and F. You, "A fragile digital watermark used to verify the integrity of vector map," 2009. doi: 10.1109/EBISS.2009.5137869.
[30] M. R. Mouhamed, A. M. Rashad, and A. Ella Hassanien, "Blind 2D vector data watermarking approach using random table and polar coordinates," 2012. doi: 10.1109/URKE.2012.6319586.
[31] Y. Li and L. Xu, "A blind watermarking of vector graphics images," 2003. doi: 10.1109/ICCIMA.2003.1238163.
[32] Z. Junfeng and X. Bing, "Research on digital watermarking algorithms for 2D graphics," 2011. doi: 10.1109/ICCSN.2011.6013689.
[33] C. Men, L. Cao, and J. Sun, "A perception-based reversible watermarking algorithm for 2D-vector maps," *Gaojishu Tongxin/Chinese High Technology Letters*, vol. 20, no. 4, 2010, doi: 10.3772/j.isan.1002-0470.2010.04.003.

[34] D. Xu and Q. Wang, “The study of watermarking algorithm for vector geospatial data based on the phase of DFT,” in *2010 IEEE International Conference on Wireless Communications, Networking and Information Security*, 2010, pp. 625–629. doi: 10.1109/WCINS.2010.5541855.
[35] S. Zope-Chaudhari and P. Venkatachalam, “Protecting geospatial data using digital watermarking,” in *2012 International Conference on Computer and Communication Engineering (ICCCE)*, 2012, pp. 594–598. doi: 10.1109/ICCCE.2012.6271256.
[36] X. Xi, X. Zhang, Y. Sun, X. Jiang, and Q. Xin, “Topology-Preserving and Geometric Feature-Correction Watermarking of Vector Maps,” *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2973458.
[37] N. Ren, Q. S. Wang, and C. Q. Zhu, “Selective authentication algorithm based on semi-fragile watermarking for vector geographical data,” 2014. doi: 10.1109/GEOINFORMATICS.2014.6950830.
[38] S. N. Neyman, B. Sitohang, and F. Cahyono, “An improvement technique of fragile watermarking to assurance the data integrity on vector maps,” in *2013 International Conference on Computer, Control, Informatics and Its Applications (IC3INA)*, 2013, pp. 179–184. doi: 10.1109/IC3INA.2013.6819170.
[39] A. M. Abubahia and M. Cocea, “Exploiting vector map properties for GIS data copyright protection,” in *Proceedings - International Conference on Tools with Artificial Intelligence, ICTAI*, 2016, vol. 2016-January. doi: 10.1109/ICTAI.2015.89.
[40] N. Ren, C. Zhu, D. Tong, W. Chen, and Q. Zhou, “Commutative Encryption and Watermarking Algorithm Based on Feature Invariants for Secure Vector Map,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3043450.
[41] AutoCAD, “Dxf reference.,” 2007.

BIBLIOGRAPHY OF AUTHORS

Hartanto Tantriawan is a lecturer at Institut Teknologi Sumatera and Doctoral Student at School of Electrical Engineering and Informatics ITB. He focuses on the research field of Digital Watermarking and Steganography.

Rinaldi Munir is a lecturer at School of Electrical Engineering and Informatics ITB. He focuses on the research field of Cyber Security and Steganography.