TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 1, February 2020, pp. 500~510
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i1.15020

RST invariant watermarking technique for vector map based on LCA-transform

Saleh AL-ardhi, Vijey Thayananthan, Abdullah Basuhail
Faculty of Computing and Information Technology (FCIT), King Abdulaziz University, Jeddah, Saudi Arabia

Article Info

Article history:

Received May 19, 2019
Revised Dec 4, 2019
Accepted Dec 19, 2019

Keywords:

Copyright protection
Geometric attacks
Linear cellular automata transform (LCAT)
Transform watermarking,
Vector map

ABSTRACT

The dangers of copyright protection can impact 2D vector maps, having a knock-on effect on the use of vector data. To achieve invariance property, uniform RST (rotation, scaling and translation) and disguising the digital vector map's information by implementing distortion control, is all done by using watermarking schemes. Convert an original map, then engrain the watermark. An LCA algorithm is used in this study, as a newly proposed way to protect the vector maps under copyright. The procedure is operated in this order: 1) use an original map, altered by the LCA algorithm, 2) use the coefficient of the transformation to engrain the watermark, inserting the resulting frequency into the LSB wave, 3) the watermarked map is acquired by using the inverse LCA map transformation. Further investigations discovered that the necessary standards of fidelity and invisibility can be achieved using this technique. This procedure also gives out numerous frequency domains for digital watermarking; as well as being resilient to signal and geometric invasions.

Corresponding Author:

Saleh AL-ardhi,
Faculty of Computing and Information Technology (FCIT),
King Abdulaziz University, Jeddah, Saudi Arabia
Email: s_ardhi@hotmail.com

1. INTRODUCTION

From the making of paper maps to digital data types, we have seen the progression of geospatial data over the past decades. Improvements in computer hardware relative to geographic data collection tools have caused this. Its proficiencies include GPS (geographic positioning systems) with satellites able to retrieve trusted spatial positioning data. The functions of analog data or print has been replaced by vector maps as the standard data units in GIS (geographic information systems) [1]. An essential component of GIS are vector maps, a type of GIS spatial data with many distinctive qualities, covers many areas from navigation to traffic data. Current investigations intend to copyright protect the owners of these systems, as they become more popular and used across the board. In comparison to multimedia data which has fixed relative positions, graphics have several independent components. Graphics can also make copying scarce due to its abundance of topology and engineering information. The incentive for research into DW (digital watermarking) for digital vector maps, can be formed from combining these factors [2].

Deciding on who owns the digital map and whether it has validity, is determined by the digital map stakeholders, due to DW. Alteration when the media point is altered and protection against data extraction are the robust benefits of DW. Robust DW for map vectors can be used on both the transformation and spatial domains, and a strong DW application can be classed as copyright protection [3]. Discrete wavelet transform (DWT) [4], discrete cosine transform (DCT) [5], and fast fourier transform (FFT) [6] are all included in

the principal transform algorithms. The convenient application of the spatial domain is at the expense of robustness and invisibility, therefore to copyright applications, robust DW procedures concentrate on the transformation domain [7-9].

Research on robust DW algorithms in the transformation domain is focused on images [10-15] and audio [16-20]. Vector maps differ from multimedia data because they are not limited to functions with integers, however different methods are needed to enter data into a vector map. IWT (integer wave transform) [21], DFT [2] and DCT [22, 23] can be used by robust DW in the vector map transformation (as proof has shown), therefore our new procedure is compared to the DWT, DCT and FFT techniques in the current investigation. For each co-ordinate sequence, the final 12 digits of the decimal are taken and then put into a matrix: (a) then altered into 4 bands, (b) different vector data methods associated with copyright digital maps have been examined, [24-26] including changeable watermarking in the spatial domain and [27] watermarking in the spatial topology domain. The progression of copyright protecting vector maps is the aim of this research. Implementation of the LCA transformation algorithm is the advanced technique for watermarking vector maps, as suggested by this paper. Multimedia watermarking has been using cellular automata transform (CAT) for a very long time [28-30]. Embedded media still has no research results in connection to its use on vector maps. Using the LCA algorithm has the benefits of high fidelity, great insertion results and high invisibility [31]. Data verification traits are present due to the use of the scrambling method [25], plus it is not limited to one transformation plane, making it unique. This sets it above the current frequency watermarking methods and it is able to accelerate DW via its multi-frequency domains.

Our methods for the performance measurements used were: 1) NC calculation was used to measure the performance technique, 2) evaluation of quality, based on invisibility with RMSE calculations, 3) fidelity with the longest distance, 4) Resistance and NC calculation against geometric attacks (e.g. RST). The new method functioned well, as is evident in the results of the invisibility test, which produced map test data RMSE values. NC data and distance change were within the accepted threshold, so map fidelity was high. There was a high level of resilience against geometric attacks, especially for the watermark as integrity was essential. There are four extra sections at the end of this paper. An explanation of the investigation procedures used in this paper are documented in section 2, followed by the results in section 3, then section 4 has a conclusion of the study.

2. RESEARCH METHOD

2.1. Linear cellular automata

A dynamical in a discontinuous frequency and time frame, symbolized by the LCA transform is shown below in (1). Each cell has a restricted group of states and form a lattice structure. Effectual and fast calculations of the discrete transformation are enabled by the algorithm [31].

$$(C^{t+1})^T = M_n.(C^t)^T (\text{mod } 2) \quad (1)$$

M_n represents the local transition matrix, given that $n = 5$ k:

$$M_n = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \dots \dots \dots \dots 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \dots \dots \dots \dots 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \dots \dots \dots \dots 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \dots \dots \dots \dots 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \dots \dots \dots \dots 0 & 0 & 0 \\ & & & & \dots \cdot \cdot & & \\ & & & & \dots \cdot & & \\ 0 & 0 & 0 & 0 & 0 \dots \dots \dots \dots 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \dots \dots \dots \dots 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \dots \dots \dots \dots 1 & 1 & 1 \end{pmatrix}$$

if the transition matrix of a cellular automation (An) was represented by M_n, the non-zero coefficients will become 1 as An is now the nth order penta-diagonal matrix. $(C^t)^T$ on the other hand, is a transposition of a linear matrix, composed of inter-changing and random binary numbers are shown in (2).

$$(C^t)^T = M_n^{-1}.(C^{t+1})^T (\text{mod } 2) \quad (2)$$

The formula below is transition matrix for the reverse of An, given that $n = 5$ k:

$$M_n^{-1} = \begin{pmatrix} M_5^{-1} & B & B & \cdots & B \\ B^T & M_5^{-1} & B & \ddots & \vdots \\ B^T & A^T & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & M_5^{-1} & B \\ B^T & \cdots & B^T & B^T & M_5^{-1} \end{pmatrix},$$

where

$$M_5^{-1} \begin{vmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{vmatrix} (\text{mod } 2),\ B = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

$|M_n| \text{mod} 2$, representing the transition matrix starts with five numbers are shown below in (3).

$$|M_n| \text{mod} 2 = \begin{cases} 1, & \text{if } n = 5k \text{ or } n = 5k+1, \text{with } k \in N \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

2.2. Linear cellular automata transform

This investigation involved doing the watermark embedding process on the vector map, which included the transformation frame of the coordinates of the vertices. This procedure was used on the coefficient of the transformation result frequency of the vector map's data. Figure 1, shows that the coordinates are converted into an LCA transform, so that the vector map can be translated into the frequency domain of a signal. This is further supported by (4), which shows that the LCA transform, can convert the host map's v_{x1} coordinate.

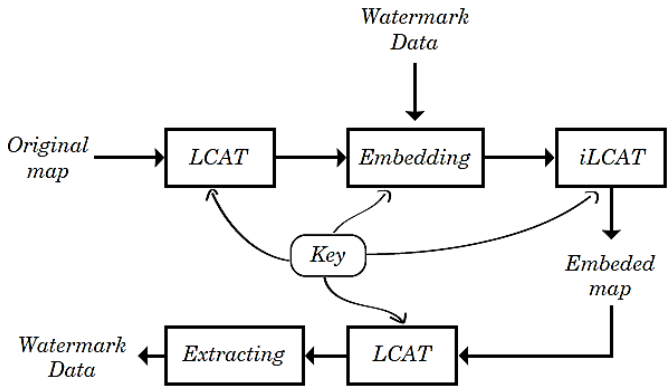


Figure 1. Visualization of LCA transform

$$T(M) = \sum_{n=0}^{N-1} M_n . v_{x1} \ (mod\ 2) \quad (4)$$

where, T(M)=host map's domain transformation value, M_n = LCA's transition matrix, v_{x1} = host map^' s digital media value, N = number of vertices altered by the frequency domain.

Note: in (5) shows that the v_{x1} co-ordinate undertakes transformation with the LCA transform, allowing for the encrypted watermark part to be put into the equation N , N , v_{x1} , $T(M)$, M_n.

$$v_{x1}'' = v_{x1}' + \alpha W \quad (5)$$

where, α=embedding parameter, W=watermark part.

Variations of the vector map are directly proportional to the embedding parameter (α), meanwhile the watermark's (W) resistances rises. This equation uses acceptable alterations to the vector map, a huge resistance value and 3-part α values. The inverse of the LCA transform is given in the following (6):

In 6 below, represents the LCA transform's inverse: v_{x1}'' , $iT(M)$

$$iT(M) = \sum_{n=0}^{N-1} M_n^{-1}.v_{x1}'' \pmod 2 \quad (6)$$

where: $iT(M)$ = host map's inverse domain transformation value , v_{x1}'' = digital media value of thehost map's transformation.

2.3. Watermark embedding phase

The suggested scheme is applied in the frequency domain and the digital watermark's embedded model is represented in Figure 2. The watermark insertion process consists of three steps, when a public key is used to encrypt (three parts, namely a vector map, the size of LCA transition matrix (Mn) and a watermark that scrambles the elements) and when a private key is used to decrypt. The proposed scheme relies on the linear cellular automata transform (LCAT) algorithm, and it operates in the frequency domain. Additionally, the proposed scheme does not fall under geometric attacks, namely, translation, scaling, and rotation. The algorithm of the scheme is as follows:

Figure 2 displays the recommended scheme, used in the digital watermark's embedded model and the frequency domain. There are three key steps to watermark insertion; when a public key is used to encrypt namely the size of Mn, watermark that mixes up elements and a vector map. This can happen when a private key is used to decrypt. This program operates in the frequency domain and depends on the LCAT (linear cellular automata transform) algorithm. The program is also is not susceptible to RST (Rotation, Scaling and Translation), which are considered to be geometric attacks. The algorithm goes like this:

- Select two reference vertices, v_{f1} and v_{f2} in the range $(1 \leq v_{f1}, v_{f2} \leq n)$ as the vector map of M, in order to assure security.
- When length (N) is transformed into a domain frequency (with no references), decide on the number of vertices in the map file (M).
- Co-ordinates fare taken from the vertex and converted into a LCAT transform
- Using equation 25, encrypt the factors of W^*, which produces the data sequence $W^* = \{w_i^* \mid w_i^* \in \{0, 1\}, i = 0, 1,...., l-1\}$
- Put W^* into the final two consecutive digits (reduces the impact on the precision) and assume that a double floating point 16-digit coordinate value in a decimal fractional version. The embedded value is in the range of 0 to 99 and does not correlate with w_i^*. If we assume that the integer D is composed of the two digits, then:

$$W^* = \begin{Bmatrix} \text{if } w_i^* \text{ is } 0 \text{ then } D \leq 50 \text{ and saved at the positions;} \\ w_i^* = 1, \text{otherwise} \end{Bmatrix} \quad (7)$$

- The initial shape file (with the inverse LCAT) of the frequency domain vector map is reinstated after the watermark is placed.

2.4. Watermark extracting phase

The watermark extraction point and the insertion process have similar steps, but in the opposing sequence. The three steps used in the exertion process are the results of the insertion process, namely the two reference vertices vf1 and vf2, fixed size LCA transition matrix (Mn), and the watermarked vector map, as shown in Figure 3. In the opposite sequence, the watermark insertion procedure and extraction point have comparable phases. The outcome of the insertion procedure, produces three steps for the exertion procedure. The results are Mn (fixed size LCA transition matrix), watermarked vector map Figure 3 and two reference vertices (vf1, vf2).

- Select v_{f1} and v_{f2} $(1 \leq v_{f1}, v_{f2} \leq n)$, under private key k's control, as the reference vertices for the vector map of M
- Determine the number of vertices in the map file M and the length (N) that will later be transformed into a domain frequency without the references
- Once the set of coordinates for each feature is obtained, it will be transformed into a *LCAT* transform
- The embedded watermark location and watermark bits are extracted using (8):

$$W^* = \begin{Bmatrix} \text{if } D \leq 50 \text{ then } w_i^* \text{ is } 0 \\ w_i^* = 1, \text{otherwise} \end{Bmatrix} \quad (8)$$

- Extract the original embedded watermark sequence W, with private key k, by inversing the watermark pattern.
- Get the watermark by rebuilding the watermark pattern.

- Select two reference vertices, v_{f1} and v_{f2} in the range $(1 \leq v_{f1}, v_{f2} \leq n)$ as the vector map of M, in order to assure security.
- When length (N) is transformed into a domain frequency (with no references), decide on the number of vertices in the map file (M).
- Co-ordinates of each feature are gained and then taken from the vertex and converted into a LCAT transform.
- The (8) is used to extract the embedded watermarked parts and location.

$$W^* = \begin{Bmatrix} \text{if } D \leq 50 \text{ then } w_i^* \text{ is } 0 \\ w_i^* = 1, \text{otherwise} \end{Bmatrix} \quad (8)$$

- Reverse the watermark pattern, so that you can use the private key (k) to extract the original embedded watermark sequence (W).
- Reconstruct the watermark pattern, in order to get the watermark.

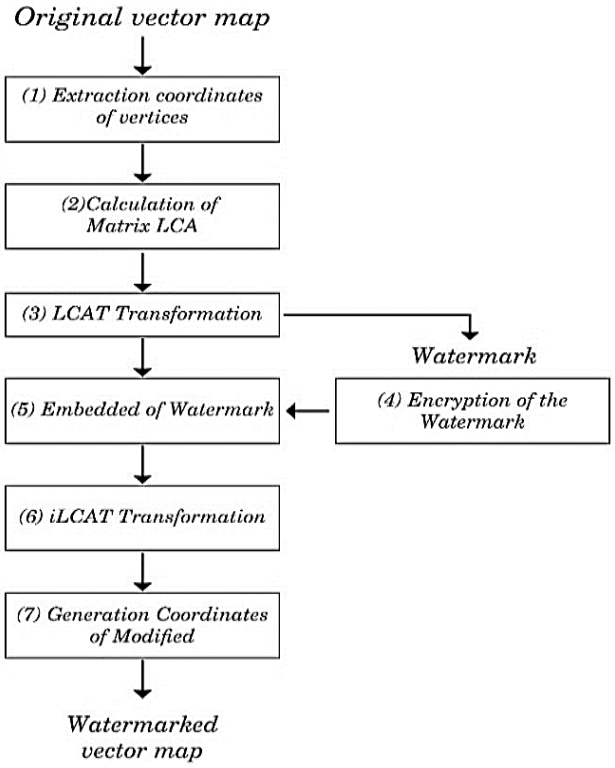


Figure 2. Watermark embedding

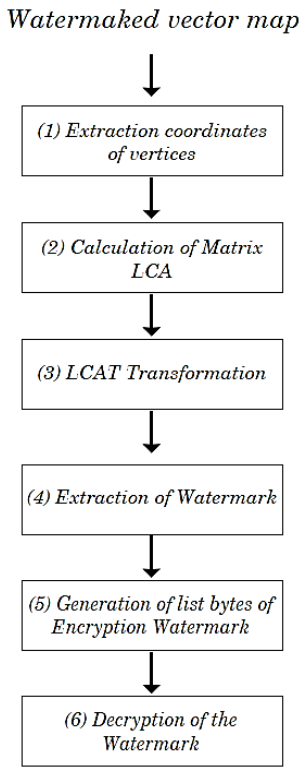


Figure 3. Watermark extraction

3. RESULTS AND DISCUSSION

3.1. Experimental results

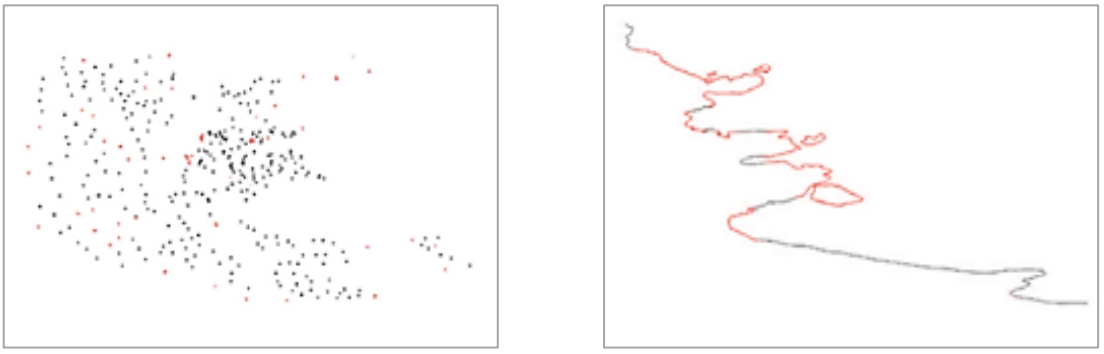
For the evaluation of data type (.shp), there are two shapefile maps. Two vector maps make up the file type ESRI standard [32], which are a spot height and coastline map of Taylor Rookery [33]. Copyright marker was represented by a bitmap picture. The PC used for this study was Windows 10 professional, QGIS version 3.0, 16 GB memory and 2.3 GHz. Programs used were python and MATLAB. The secret parts associated with each transform coordinate had a $M_n = 30$, α in LSB and $T = 1$ for iterative embedding. The invisibility of our approach was displayed in the first test. Figure 4 shows vector maps watermarked, using the method suggested in section 3.5. This produced the watermarked types displayed in Figure 5.

The recommended performance technique analysis for this study was measured by the NC calculation. It was also used to examine the similarities between the original watermark, before and after the extraction (values ranging 0-1). The success of the watermarking usage is indicated by how high the NC

value is. The larger the NC value is, the more similarity there is between images. In (9), w (initial value) and w_i^* are the extracted watermarks. Table 1 shows that the original and extracted watermarks are the same, as the evaluation result for NC is approximately 1, plus they have the same watermark content and length. This procedure was able to input copyrights as a watermark (without lessening its quality), as a watermark extracted again from the vector map file, does not need to go through dimensions or content changes.

(a) (b)

Figure 4. Test 2D vector maps: (a) spot height map of Taylor Rookery, (b) coastline map of Taylor Rookery



(a) (b)

Figure 5. The watermarked 2D vector maps of Figure 4 map

$$NC = \frac{\sum_{i=0}^{M} w_i \ X \ w_i^*}{\sqrt{\sum_{i=0}^{M}(w_i)2} \ X \ \sqrt{\sum_{i=0}^{M}(w_i^*)2}} \quad (9)$$

Table 1. Result of similarity test between original watermarks and extracted watermark

Map	Map Type	Features/vertices	Original Watermark	Extracted Watermark	NC
a	Point	355/355			0.998909
b	Polyline	18/4279			0.998308

3.2. Invisibility evaluation

Table 2 shows the two parameters that were used previously in the invisibility measurement (as reference analysis for calculating RMSE), which subsequently decides on the alteration between

the interpolated watermark's results and the beginning of the map file. The equation for the making of the RMSE, is shown below: N , v $_{x1}{}^{*\prime\prime}$

$$\text{RMSE} = \left(\frac{1}{N_V} \sum_{i=0}^{N_V} |v_i - v_i{}^{*\prime\prime}|\right) \quad (10)$$

where, N =the number of vertex map vectors, v_{x1} =equivalent x coordinates in the initial vector map. $v_{x1}{}^{*\prime\prime}$ = equivalent x coordinates in the recovered vector map.

Table 2. RMSEs between the recovered maps and the original maps ($\times 10^{-9}$) (T = 1)

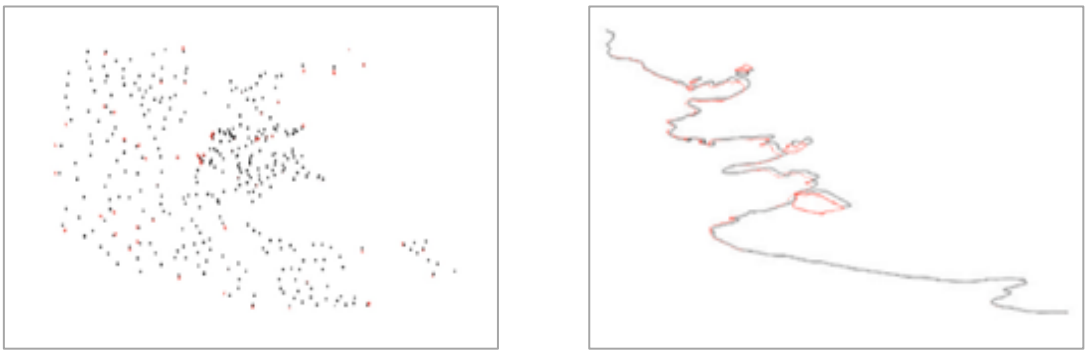
Map	DCT	DWT	FFT	Proposed (LCAT)
a	5.0917×10−4	1.3014×10−4	2.9023×10−5	1.1317×10−9
b	1.8514×10−3	3.5872×10−4	2.3342×10−5	3.1562×10−9

3.3. Fidelity evaluation

Digital watermarking is untraceable by human senses, making it a very reliable system, plus it doesn't significantly worsen the media file interpolation. Moreover, with regards to RMSE, the furthest changes can be gauged. A position change is indicated by the furthest distance, which is caused by watermark interpolation into vector files. This is gained via an assessment comparing the original vector map file, vector map file (containing the watermark) and coordinated vertex. To convert the furthest distance into meters, QGIS is implemented. The lengthiest noticeable shift in data analysis is 60 cm, as seen in Table 3, therefore the furthest distance value still maintains a significance level of precision in the vector map, which is displayed in Figure 6.

Table 3. Result of fidelity test between original maps with watermarked mas

Map	τ (m)	DCT	DWT	FFT	Farthest Distance (meter) LCAT
a	0.5	0.45	0.4	0.3	0.050
b	0.5	0.5	0.43	0.38	0.068



(a) (b)

Figure 6. Original and watermarked map overlaid with each other

3.4. Robustness evaluation

Examining the strength of the watermark is the next stage. Advanced methods are used to challenge the three geometric attacks, classed as RST (rotation, scaling and translation). The RST also includes a signal operation attack of three components; vertex deletion, vertex modification and vertex insertion. Attacks in the form of a vertex point embedded in watermarks and vector maps with spatial features, were used to test on the data. In order to conduct attacks on the test vector maps, QGIS software is used and the results of the extraction to determine the impact of the attacks Table 4, are found out by doing NC calculations. Table 4 can be distinguished into three parts: 1) Rotation attack: rotating the test data coordinates by 30° to 180°, 2) scaling attack: enlarging the test map from 0.25 to 4.0, and 3) translation attack: Alter the positioning of the vertices by moving the coordinates.

Table 4. Experiment results for robustness

Attack Type	Detection Rate (NC)
Rotation (ρ=30°)	0.939542
Rotation (ρ=60°)	0.921861
Rotation (ρ=90°)	0.906505
Rotation (ρ=180°)	0.898085
Scaling (ς = 0.25)	0.913221
Scaling (ς = 0.5)	0.890227
Scaling (ς = 2.0)	0.884843
Scaling (ς = 4.0)	0.880051
Translation (−1.2 m, -2.3 m)	0.901241
Translation (4.2 m , 5.6 m)	0.896940
Translation (2.6 m, – 7.9 m)	0.765425
Translation (– 0.6 m, 0.7 m)	0.558168

3.4.1. Rotation attack

Turning a vector map, in order to reduce the WDR (Watermark Deduction Rate) is the definition of rotation. Figure 7 shows that there was a rotation from ρ=30° (low point) to ρ=180° (high point). Only very small effects on the quality of the embedded watermark were shown by the testing. We now have evidence that the recommended WV map is sufficient enough to resist such an attack.

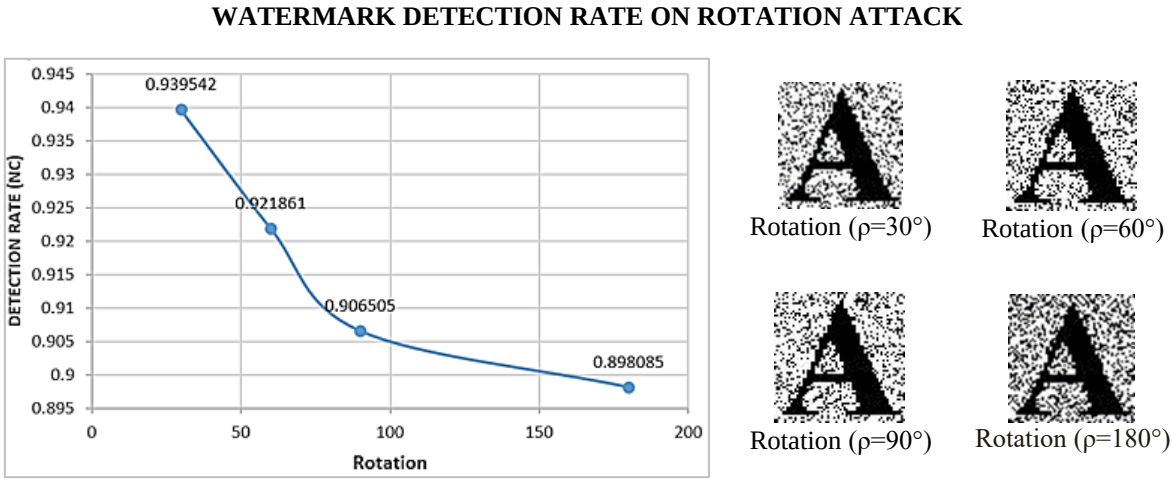


Figure 7. Quality of watermark vector map after rotation attacks

3.4.2. Translation attack

Scaling (for this study), is defined as resizing a map along its axes, so that the WDR can be reduced. The scaling range was ς = 0.25 (low) to ς = 0.25 (high). Akin to the rotation attacks, scaling attacks also have only a small impact on the WDR and Figure 8 shows that the watermark embedded, just about managing to survive. We can conclude that under a scaling attack, this method of LCAT watermarking is only modestly robust.

3.4.3. Translation attack

Relocating the whole map shifting it into a specific direction, is the main trait of the translation attacks. The map used in this research, translated from -1.2, -2.3 m to -0.6 m, 0.7 m in Figure 9. The studies only showed a minor effect on the quality of embedded watermark, apart from the exceptions at -7.9, -0.6 m, 0.7 m, and 2.6. The minimal impact could be due to the translation attacks, so we can conclude that the LCAT watermarking technique is moderately resistant to translation attacks. Watermark extraction was not always attained, by the attack techniques (with NC=1). Out of the entire evaluation scenario, the failure rate of the watermark detection was 89%. From this, we know that these extraction methods can't be used in attacks that change the watermark bit (Table 4). Friction against the vertex is made by TAs, changing the WBV (Watermark Bit Value) and stopping extraction. In the meantime, rotation attack results show that the watermark extraction will be unsuccessful is the bit value changes by up to 1. If the LCAT algorithm can't maintain its fixed genuine watermark level during an attack, then the WBV changes and extraction becomes unattainable.

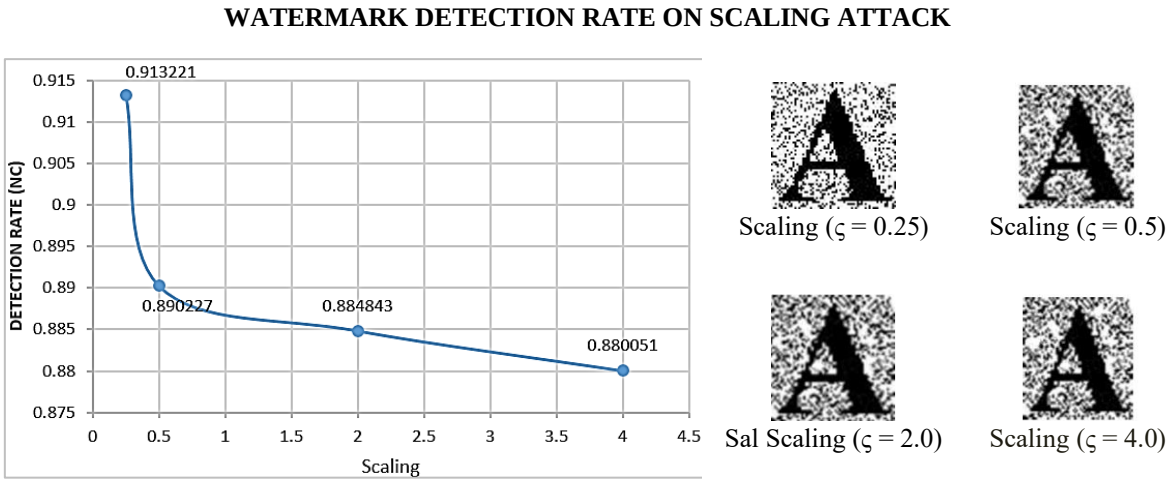


Figure 8. Quality of watermark image after scaling attacks

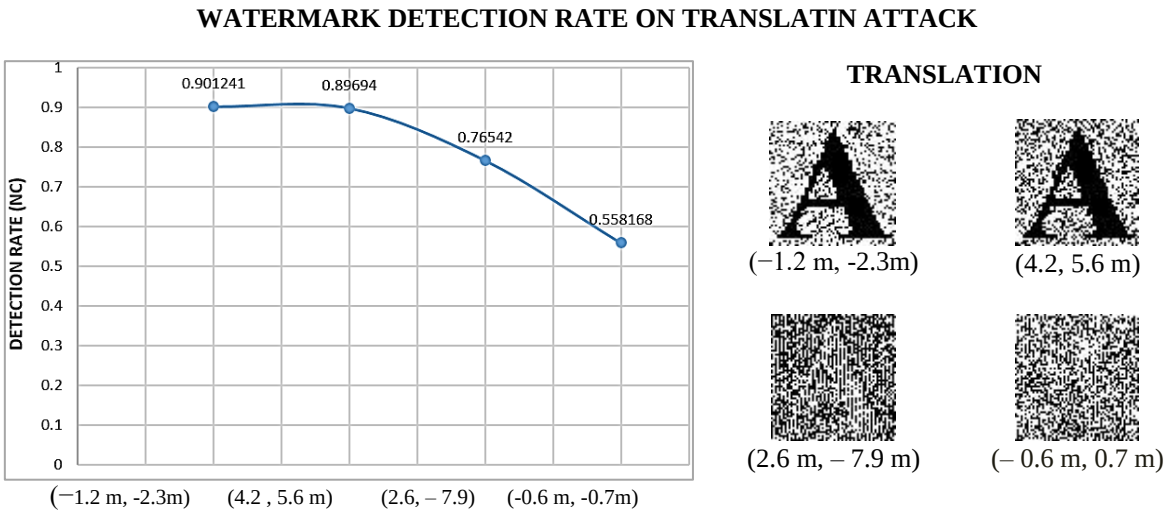


Figure 9. Quality of watermark vector map after translation attacks

3.5. Comparative study of watermarking techniques

There are various watermarking techniques describes in this study. When they are tested on DWT, FFT and DCT algorithms; fidelity, geometrical attacks and better invisibility is shown by the linear cellular automata [31]. Following this, 1D image files were watermarked by CAT; despite the fact that 2-D CA needed to be converted between two dimensions, specifically along with repetition. The same keys, vertices and maps shown in Table 5 were used, to compare them to our program [31]. Table 6 summarizes the resistance of the four techniques against the RST attacks (in relation to watermark immunity to elimination and inadvertent degradation). LCAT comes out on top, as a detection rate of 0.76; indicates that a complete watermark recovery is still feasible.

Table 5. Parameters analysis of both DCT, DWT, FFT and LCAT

Parameters analysis				
Evaluation Metrics	LCAT	DWT	FFT	DCT
Invisibility	high	medium	high	medium
Fidelity	high	Low	medium	Low
Geometrical Attacks	89%	77%	83%	74%

Table 6. Watermark detection rate comparison for DCT, DWT, FFT, LCAT under various attacks

Attack Type	DCT	DWT	FFT	LCAT
Rotation (ρ=30°)	0.87	0.85	0.88	0.94
Rotation (ρ=60°)	0.84	0.86	0.90	0.92
Rotation (ρ=90°)	0.80	0.80	0.86	0.91
Rotation (ρ=180°)	0.62	0.80	0.79	0.90
Scaling (ς = 0.25)	0.47	0.62	0.72	0.91
Scaling (ς = 0.5)	0.65	0.70	0.78	0.89
Scaling (ς = 2.0)	0.87	0.90	0.93	0.88
Scaling (ς = 4.0)	0.78	0.73	0.84	0.88
Translation (−1.2 m, -2.3 m)	0.77	0.83	0.88	0.90
Translation (4.2 , 5.6)	0.82	0.83	0.87	0.90
Translation (2.6, – 7.9)	0.71	0.73	0.80	0.85
Translation (-0.6 m, -0.7 m)	0.68	0.60	0.67	0.76

Manipulation of results on the watermark insertion map, is the cause of watermark extraction failure. The distortion value is affected by the use of the limitation value in the watermark insertion. The watermark value is found by using a bit matrix size of $M_n \leq 30$, in order to allow for extraction. Limitation value is affected by modification amplitudes of $M_n \geq 35$ bits. The techniques of some of the tests, managed to keep the same watermark, extracted and original watermarks were the same and NC = 1, in spite of the low robustness. For every LCAT value, modifications on the value of the sequence complex on the vector mapping, an LCAT calculation was spread for each one. This was done to keep the LCAT value within the limits of the watermark extraction. Alterations to the coordinate value, directly affects the inserted watermark bit value; when insertion happens on the spaced-out domain. This will produce contrasting results. The transform domain calculation spanning the LCAT is better at conserving the watermark, in comparison to the spatial technique. The robustness of the method depends on, FDA (frequency domain algorithm), extraction limit, related programming methods, asymmetric algorithm key quality and the data storage length.

4. CONCLUSION

Finding a good frequency watermarking scheme for 2D vector map drawings was the principal aim of this paper. The frequent problems with watermarking schemes of vector maps are invisibility, high fidelity and weak robustness. Furthermore, the scheme needs the original cover when extracting the watermark, because it is 'Non-blind'. A watermarking technique (that was LCAT domain transformed) was embedded into the vector map. Invisibility showed that likeness in fidelity stages, in the watermarked map are upheld. The RMSE (distortion scale) staying circa zero and the distance from the original vector map being 10% or less, also displayed this. The impact of the frequency domain scatters throughout various frequencies, restraining impact and upping this method's dependability. LCAT FDA warrants the vector map's exactness and robustness is shown in 89% of examined cases.

REFERENCES

[1] K. T. Chang, "Introduction to Geographic Information Systems," McGraw-Hill, 2012.
[2] V. Tao, X. Dehe, L. Chengming, and S. Jianguo, "Watermarking GIS Data for Digital Map Copyright Protection," Proceedings of the *24th International Cartographic Conferences (ICC)*, pp. 1-9, 2009.
[3] A. Abubahia, and M. Cocea, Advancements in GIS Map Copyright Protection Schemes-a Critical Review," *Multimedia Tools and Applications*, vol. 76, no. 10, pp. 12205-12231, 2017.
[4] Y. Ling, C. F. Lin, and Z.Y. Zhang, "A Zero-Watermarking Algorithm for Digital Map Based on Dwt Domain," *Computer, informatics, cybernetics and applications*, vol. 107, pp. 513-521, 2012.
[5] J. Wu, Q. Liu, J. Wang, L. and Gao L, "A Robust Watermarking Algorithm for 2D CAD engineering graphics Based on Dct and Chaos System," *Advances in swarm intelligence*, vol 7929, pp. 215-223, 2013.
[6] S.N. Neyman, I. N. P. Pradnyana, and B. Sitohang, "A New Copyright Protection for Vector Map Using fft Based Watermarking," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 12, no. 2, pp. 367-337, 2014.
[7] S. AL-ardhi, V. Thayananthan, and A. Basuhail. "Copyright Protection and Content Authentication Based on Linear Cellular Automata Watermarking for 2D Vector Maps," *Advances in Computer Vision CVC 2019*, pp. 700-719, 2019.
[8] S. AL-ardhi, V. Thayananthan, and A. Basuhail, "Fragile Watermarking based on Linear Cellular Automata using Manhattan Distances for 2D Vector Map," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 6, 2019.
[9] S. AL-ardhi, V. Thayananthan, and A. Basuhail, "A Watermarking System Architecture using the Cellular Automata Transform for 2D Vector Map," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 6, 2019.

[10] Y. Xu, Q. Zhang, and C. Zhou, "A Novel DWT-Based Watermarking for Image with The SIFT," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 11, no, 1, pp. 191-198, 2013.
[11] H. Gao, L. Jia, and M. Liu, "A Digital Watermarking Algorithm for Color Image Based on DWT," *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 11, no. 6, pp. 3271-3278, 2013.
[12] C. Ma, Y. Zhu, M. Chi, and Yongyong, "A Novel Selfadaptive Discrete Wavelet Transform Digital Watermarking Algorithm," *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 11, no. 11, pp. 6281–6289, 2013.
[13] J. Li, Q. Cao, "DSDWA: A DCT based Spatial Domain Digital Watermarking Algorithm," *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 12, no. 1, pp. 693-702, 2014.
[14] H. Suryavanshi, A. Mishra, and S. Kumar, "Digital Image Watermarking in Wavelet Domain," *International Journal of Electrical and Computer Engineering*, vol. 3, no. 1, pp. 1-6, 2013.
[15] Q. Liu, "An Adaptive Blind Watermarking Algorithm for Color Image," *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 11, no. 1, pp. 302-309, 2013.
[16] A. Al-haj, A. Mohammad, and L. Bata, "DWT–Based Audio Watermarking," *Int. Arab J. Inf. Technol*, vol. 8, no. 3, pp. 326-333, 2011.
[17] P. K. Dhar, and J. Kim, "Digital Watermarking Scheme Based on Fast Fourier Transformation for Audio Copyright Protection," *Int. J. Secur. Its Appl*, vol. 5, no. 2, pp. 33-48, 2011.
[18] I. H. Sarker, M.I. Khan, K. Deb, and M. F. Faruque, "FFT-Based Audio Watermarking Method with a Gray Image for Copyright Protection," *Int. J. Adv. Sci. Technol*, vol. 47, pp. 65-76, 2011.
[19] A. Tefas, A. Giannoula, N. Nikolaidis, and I. Pitas, "Enhanced Transform-Domain Correlation-Based Audio Watermarking. Proceedings (ICASSP '05)," *IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 2, no. 2, pp. 1049-1052, 2015.
[20] K. B. Vivekananda, I. Sengupta, and A. Das, "Audio Watermarking Based on Quantization in Wavelet Domain," *In Information Systems Security Sekar R and Pujari A K (eds) Springer*, Berlin Heidelberg, pp. 235-242, 2008.
[21] C. Zhu, C. Yang, and Q. Wang, "A Watermarking Algorithm for Vector Geo-Spatial Data Based on Integer Wavelet Transform," The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, vol. 37, pp. 15-18, 2008.
[22] B. Liang, J. Rong, and C. Wang, "A Vector Maps Watermarking Algorithm Based On DCT Domain," *ISPRS Congr*, vol. 28, no. 3, 2010.
[23] A. Li, W. Zhou, B. Lin, and Y. Chen, "Copyright Protection for GIS Vector Data Production," *Proceedings of SPIE*, vol. 7143, 2008.
[24] A. Li, B. Lin, Y. Chen, and G. Lü, "Study on Copyright Authentication of GIS Vector Data Based on Zero-Watermarking," *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol 28. pp. 1783-1786, 008.
[25] N. Wang, H. Zhang, and C. Men. "A High Capacity Reversible Data Hiding Method for 2D Vector Maps Based on Virtual Coordinates," *Comput Aided Design*, vol. 47, pp. 108-117, 2014.
[26] L. Cao, C. Men, and R. Ji, "Nonlinear Scrambling-Based Reversible Watermarking for 2D-Vector Maps," *Visual Computer*, vol. 29, no. 3, pp. 231-237, 2012.
[27] C. Wang, Z. Peng, Y. Peng, L. Yu, "Watermarking 2D Vector Maps on Spatial Topology Domain," *International Conference on Multimedia Information Networking and Security*, vol. 71-74, 2009.
[28] R. Shiba, S. Kang and Y. Aoki, "An Image Watermarking Technique using Cellular Automata Transform," *TENCON 2004 IEEE Region 10 Conference*, pp. 303-306, 2004.
[29] A. Dalhoum. *et al*, Digital Image Scrambling using 2D Cellular Automata," *IEEE Multimedia*, 2012.
[30] R. Shiba, S. Kang and Y. Aoki, "An Image Watermarking Technique using CAT," *2004 IEEE Region 10 Conference*, vol. 1, no. 303-306, 2004.
[31] A. M. D. Ray and G. R. Sanchez, "Reversibility of Linear Cellular Automata," *Applied Mathematics and Computation*, vol. 217, no. 21, pp. 8360-8366, 2011.
[32] ESRI Shape File Technical Description. Technical Description, [Online], Available: https://www.esri.com/library/whitepapers/pdfs/shapefile.pdf, July 1998.
[33] Harris U, "Windmill Islands 1: 50000 Topographic GIS Dataset," Australian Antarctic Data Centre-CAASM Metadata, Accessed: 09 July 2012, 1999.