A Watermarking System Architecture using the Cellular Automata Transform for 2D Vector Map

Saleh AL-ardhi[*1], Vijey Thayananthan[*2], Abdullah Basuhail[*3]
Faculty of Computing and Information Technology (FCIT)
King Abdulaziz University
Jeddah, Saudi Arabia

***Abstract*—Technological advancement, paired with the emergence of increasingly open and sophisticated communication systems, has contributed to the growing complexity of copyright protection and ownership identification for digital content. The technique of digital watermarking has been receiving attention in the literature as a way to address these complexities. Digital watermarking involves covertly embedding a marker in a piece of digital data (e.g., a vector map, database, or audio, image, or video data) such that the marker cannot be edited, does not interfere with the quality or size of the data, and can be extracted accurately even under the deterioration of the watermarked data (e.g., as a consequence of malicious activity). The purpose of this paper is to describe a watermarking system architecture that can be applied to a 2D vector map. The proposed scheme involves embedding the watermark into the frequency domain, namely, the linear cellular automata transform (LCAT) algorithm. To evaluate the performance of the proposed scheme, the algorithm was applied to vector maps from the Riyadh Development Authority. The results indicate that the watermarking system architecture described here is efficient in terms of its computational complexity, reversibility, fidelity, and robustness against well-known attacks.**

***Keywords*—Digital watermarking; spatial database; 2d vector map; linear cellular automata transform**

I. Introduction

Although digital technologies have yielded numerous benefits, the unlawful use of data through piracy, counterfeiting, and copyright infringement remains a fundamental challenge. Until recently, the schemes proposed for mitigating these challenges have largely been inefficient and ineffective [1, 2]. One of the principal reasons for this relates to the fact that with suitable software, it is possible to deform, copy, and modify digitally-stored data in a relatively straightforward way.

To date, the most efficient and effective solution to this challenge is referred to as digital watermarking [3]. As a result of the technique's robustness in protecting digital copyrights, as well as other applications such as source tracking, authentication, and fraud and tamper detection, many researchers have started to investigate the topic. At its heart, digital watermarking involves inserting a marker (also known as the “hidden information”, “payload”, or “watermark”) into a piece of digital data that is amenable to watermarking (also known as a “host signal” or a “cover work”). The types of cover work are varied, ranging from images, audio and videos to vector maps and databases; while the types of watermark range from images and pieces of identification text to secret messages [4-6].

Diverse constraints are necessary for a watermarking system to function effectively. Foremost among these constraints is the requirement for the payload to be (a) undetectable and (b) resistant to replacement or removal. Another critical constraint is that the quality and size of the cover work must not be affected by the insertion of the payload. Furthermore, it is essential for the payload to remain extractable even in situations where the quality of the cover work has degraded. Lastly, the existence or non-existence of the payload must only be perceptible to the party with relevant permissions to access it (e.g., the holder of a private key).

This paper is concerned with presenting an efficient and effective digital watermarking architecture for concealing a payload within a spatial database. The proposed scheme was designed to apply especially to 2D vector maps. The scheme involves the provision of frequency domain information, where the insertion of the payload into the cover work relies on the linear cellular automata transform (LCAT) algorithm. Specifically, the coordinate is separated into the least significant digit (LSD) [7] and the most significant digit (MSD) [8] planes, where the LSD is typically found in the LSD. Given that the human eye cannot detect minor alterations in the LSD planes of 2D vector maps, the payload was concealed in the LSD zones. Additionally, the robustness of the proposed scheme in terms of its security was reinforced by utilising both a public and a private key [9].

II. Digital Watermarking

A. Definitions and Concepts

Despite the steganography dimensions of digital watermarking [10], the finality of each is distinct, and the procedures associated with each are distinguished by their roles. That is to say, steganography is concerned with the transmission of a secret message from a sender to a receiver, while digital watermarking architectures are concerned with embedding invisible payloads into cover work without undermining its quality or increasing its size.

As previously noted, digital watermarking is the best-known way to solve the problem of copyright protection for digital content. The aim of the technique is to embed an invisible and non-temporary mark in a piece of digital data that is amenable to watermarking (also known as a “host signal” or a “cover work”). The watermark must not be detectable by any party other than the data owner, and it should be resistant to all malicious attempts to extract it. When a digital watermarking process satisfies these key constraints, it can be considered robust.

Permission information relevant to the cover work is typically contained in the payload. As noted in the introduction section, document authentication applications can benefit from digital watermarking because these schemes allow data owners to confirm the integrity of the cover work [11-13]. Furthermore, a payload can be used to determine which entity is the owner of the document [14-16]. In terms of what the payload consists of when it is used for document owner identification purposes, it can be a distinctive code that specifies the author or the original purveyor of the document.

Robust digital watermarking schemes that can be deployed in real-world settings are characterised by the following characteristics: firstly, the invisibility of the payload to the human eye and, furthermore, the ability of payload insertion not to degrade or undermine the quality of the cover work; secondly, specificity (also known as unambiguity), which means that the payload must be retrievable by the detection system, and that it must provide a clear indication of the cover work owner; and finally, the resistance of the payload against common attacks (e.g., attempts to remove the payload) must be high, and any removal of the payload should undermine the cover work's quality.

B. *Watermarking System Process*

The embedding component and the recovery component are the fundamental elements of any digital watermarking system. The inputs to the embedding component are the watermark itself (w) and the cover work (c), as well as any required keys and the original map. Significantly, the embedding process in a digital watermarking system involves the utilisation of a private key. In view of this, the private key is also critical for the watermark detection component. An overview of the watermark embedding component is presented in Fig. 1, the output of which is the watermarked map.

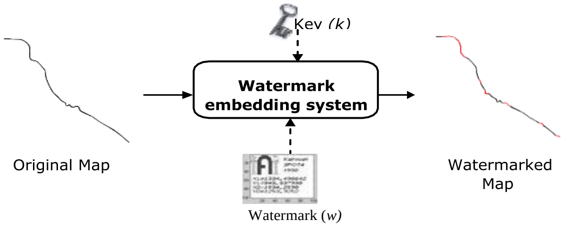


Fig. 1. Watermark Embedding Process.

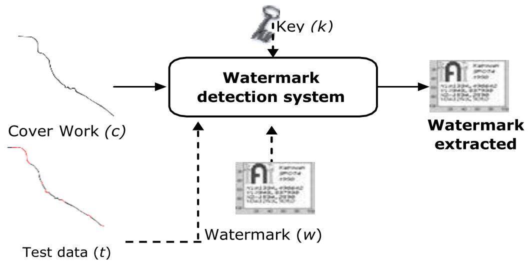


Fig. 2. Watermark Detection Process.

The recovery component of a digital watermark embedding system removes the payload from the cover work, and its inputs are the following: firstly, the test data (t), which could be distorted; secondly, the private key; thirdly, the watermark (w); and finally, the cover work (c). In the event that t was not subjected to malicious removal attempts, then the output of the watermark removal component is the extracted watermark or an indication of its presence [3], which characterises the mark presence probability. Alternatively, if t was subjected to attacks by an adversary, then nothing is outputted from the watermark removal component. An overview of watermark removal component is presented in Fig. 2.

C. *Watermarking Techniques*

Traditional digital watermarking techniques are non-complex and lack robustness, but the degree to which these techniques are complex, sophisticated, and robust has increased in recent years. The classification of a digital watermarking technique is typically based on the associated domain, where the principal domains are the following: firstly, the space domain; and secondly, the transform domain. In view of this, the two main groups of digital watermarking techniques are space domain approaches and transform domain approaches. Nevertheless, it is worth noting that some researchers differentiate between digital watermarking techniques based on the nature of the system's watermark embedding component. From this perspective, the techniques can be viewed as either additive (where the payload is added to the features of the cover work) or subtractive (where coefficients of the cover work are replaced to embed the digital watermark).

- ***Space-domain approaches:*** Space domain approaches to digital watermarking involve shifting a map's vertices inside a predetermined tolerance range, and then employing suitable embedding strategies (see the following subsection). In this case, the embedding space can be represented using polar coordinates [17], blocks [18], topological relations [19], or Cartesian coordinates [7] (see Fig. 3).

- ***Transform-domain approaches:*** Compared to space domain approaches, their transform domain counterparts greatly advance the degree to which the digital watermarking system is robust and resistant to malicious activities [5]. The embedding component of a digital watermarking system that is based on a transform domain approach first applies a transformation on the cover work. As shown in Fig. 4, this is achieved using the discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform, or fast Fourier transform (FFT) [20-22]. Following this, the watermark insertion phase begins, which is achieved by changing coefficients within the cover work to produce a transformed, watermarked version of the cover work. The final phase, which involves applying the reverse transformation to the output of the second phase, yields a watermarked version of the cover work. An overview of the watermarking process for transform domain approaches is presented in Fig. 5.

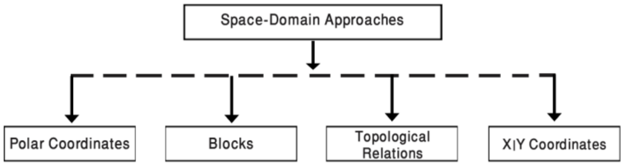


Fig. 3. The Classification Space-Domain Approach.

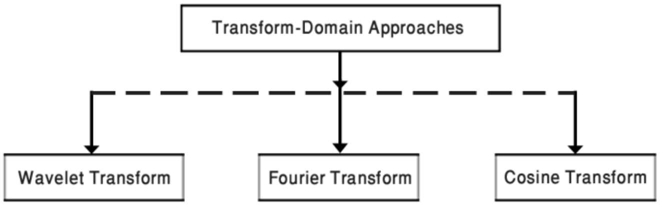


Fig. 4. The Classification Transform-Domain Approach

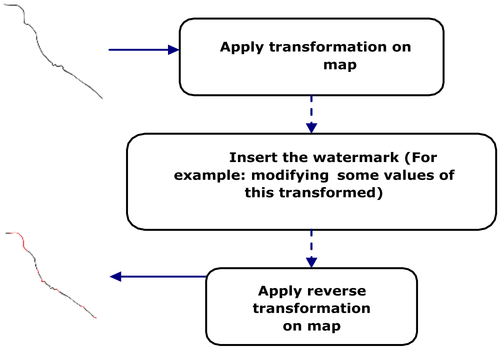

Apply transformation on map
Insert the watermark (For example: modifying some values of this transformed)
Apply reverse transformation on map

Fig. 5. General Watermarking Process in Frequency Domain.

III. Linear Cellular Automata

The linear cellular automata transform (LCAT) algorithm is employed to represent a dynamical in a frequency domain and a discrete time domain. The cellular automata are configured into regular lattice structures, each of which possesses a set of states that is limited in size. Generally speaking, LCAT is employed for rapid and efficient calculations of the discrete transformation, and one of the fundamental strengths of the algorithm relates to the fact that it can reduce complexity. LCAT can be expressed as shown in equation (1) [23].

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

where, M_n, letting $n = 5k$, is the local transition matrix given below.

$$M_n = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \ldots\ldots\ldots\ldots 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \ldots\ldots\ldots\ldots 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \ldots\ldots\ldots\ldots 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \ldots\ldots\ldots\ldots 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \ldots\ldots\ldots\ldots 0 & 0 & 0 \\ & & & & \ldots.. & & \\ & & & & \ldots. & & \\ 0 & 0 & 0 & 0 & 0 \ldots\ldots\ldots\ldots 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \ldots\ldots\ldots\ldots 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \ldots\ldots\ldots\ldots 1 & 1 & 1 \end{pmatrix}$$

Suppose that M_n is the transition matrix of An, a cellular automaton. Hence, M_n can be described as an nth order pentadiagonal, matrix for which the non-zero coefficients are 1. Where, M_n denotes the pentadiagonal matrices and $(C^t)^T$ is the transposition of a linear matrix containing varying random bits. Equation (2) states the inverse formulation of LCAT.

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

M_n^{-1}, the transition matrix for the inverse cellular automaton of An, letting $n = 5k$, can be expressed as follows:

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

where

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

As specified in equation (3), the transition matrix's size begins at 5 elements.

$$|M_n|mod2 = \begin{Bmatrix} 1, & if\ n = 5k\ \ or\ \ n = 5k+1, with\ k \in N \\ & 0, other\ wise \end{Bmatrix} \tag{3}$$

A. Linear cellular Automata Transform

The need exists for new techniques that can be used to apply digital watermarks to vector maps in a robust, attack-resistant, and efficient way, thereby promoting copyright protection performance. Therefore, this study proposes a novel digital watermarking domain transformation that can serve as proof of copyright on vector maps, which relies on the linear cellular automata transform (LCAT) algorithm. Although LCAT is widely-used in the field of digital watermarking for multimedia cover work [24, 25], it has not been previously applied to vector maps as the inserted media. For this study, the digital watermark serves as a copyright marker on the vector map, and it is applied on the transformation domain for the coordinate of the vertices. As for the process of embedding the watermark, this is used for the coefficient of the transformation result frequency of the vector map data. The modification of the vector map coordinate into an LCAT takes place in this study in order to facilitate the transformation of the vector map into a domain frequency signal. The key concept to note for the proposed scheme is that v_{x1}, the coordinate of the host map, can be transformed using LCAT. Regarding the formulation of LCAT, this is given in equation (4) (see Fig. 6).

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

where $T(M)$ represents the host map's domain transformation value, v_{x1} represents the host map's digital media value, N refers to the total number of vertices that will be modified to become a frequency domain, and $\mathrm{M_n}$ is the linear cellular automaton's transition matrix.

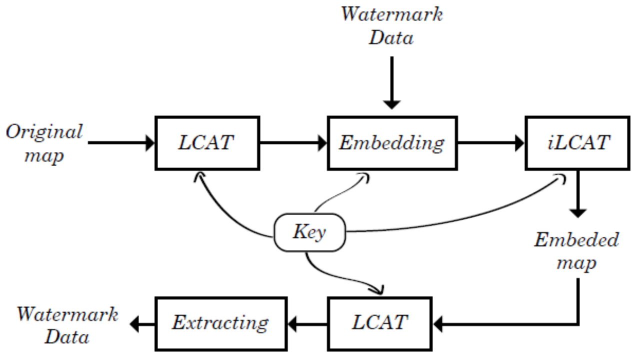


Fig. 6. The Flow Chart of the Linear Cellular Automata Transform Algorithm.

The key concept is that v_{x1}', the coordinate of the host map, is transformed using LCAT, after which the encrypted watermark bit is inserted into the cover work. Equation (5) describes the watermark insertion technique associated with the proposed scheme.

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

where W denotes the watermark bit and α represents the embedding parameter. A noteworthy feature of equation (5) is that a directly proportional relationship exists between the size of α and the extent of the modifications that will take place to the vector map file. However, the fact should not be overlooked that larger α values are associated with higher watermark resistance. In the proposed scheme, a 3-bit α value is employed, which confers satisfactory resistance and, moreover, vector map alterations that are within acceptable limits. A flow chart for LCAT is given below.

The inverse formulation of LCAT is stated in equation (6).

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

where $iT(M)$ represents the value of the host map's inversion domain transformation and v_{x1}'' denotes the host map's transform digital media value.

IV. Our Contribution

The proposed digital watermarking architecture is robust and appropriate for copyright protection, 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 depend on a previous knowledge of the cover work. This scheme is resistant to all Vertex insertion attacks, including Vertex deletion (50%) and Vertex modification (50%), and it does not fall under geometric attacks, namely, translation, scaling, and rotation

A. Proposed Architecture

As shown in Fig. 7, the architecture of the proposed digital watermarking system is separated into the following three modules: firstly, the vector map base and watermark set comprise the containing information system; secondly, the user interface is an online interface, meaning that users can straightforwardly interact with the spatial database, download existing vector maps, and consult existing vector maps; and thirdly, the watermarking system itself, which constitutes the critical component of the system, and which contains both the embedding unit and extraction unit. It should be noted that the watermarking system in this architecture contains another unit, namely, the evaluation unit, the purpose of which is to verify the watermarking process and evaluate system quality. This is achieved by following up on the output of the watermarking stage. The database owner controls the evaluation unit. For the remainder of this paper, the discussion centres around the third module of the system architecture.

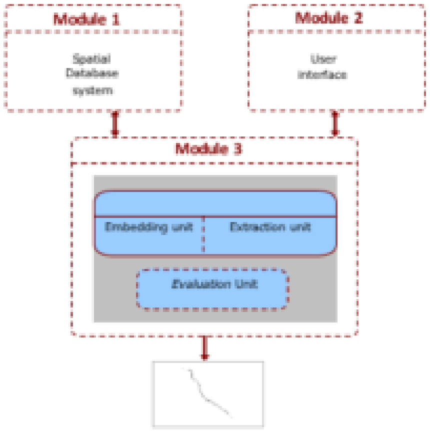


Fig. 7. Proposed Architecture.

V. Watermarking Technique

A. Embedding Scheme

The embedding unit of the proposed scheme involves the insertion of the watermark into the details (maps). Noteworthily, one of the fundamental strengths of LCAT is the way in which it guarantees the invisibility of the payload. Additionally, given that minor changes in low frequency do not register on the human visual system, the scheme embeds the digital watermark in the low frequency zones of the decomposed map. Keys were employed for the embedding and recovery phases to increase the degree to which the scheme was robust.

Fig. 8 provides an overview of the process used to embed the payload into the cover work. The steps involved in each stage of the embedding unit's algorithm are the following:

1) To serve as M's vector map, choose a pair of reference vertices v_{f1} and v_{f2}, where $1 \leq v_{f1}, v_{f2} \leq n$. This promotes the security of the embedding process.

2) Calculate the number of vertices in M, the map file, where the length (N) is subsequently changed into a domain frequency without the references.

3) Transform the coordinates collected from the vertex point using LCAT.

4) Employ the approach described in [23] for the purpose of encrypting the factors of W^*, and derive the data sequence $W^* = \{w_i{}^* \mid w_i{}^* \in \{0, 1\}, i = 0, 1, ..., l - 1\}$.

5) Posit a double floating-point number as a 16-digit coordinate value in a decimal fraction format, and then insert W^* into the final two digits. The final two digits are chosen due to the fact that these have an extremely limited impact on the scheme's precision.

It is worth noting that the inserted value does not match $w_i{}^*$, and it falls in the 0-99 range. Thus, supposing that D is the integer created by the final digits, it is possible to state the following:

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

6) Once the watermark has been embedded in the cover work, the inverse formulation of LCAT (iLCAT) is used to restore the frequency domain vector map to its original shape file.

7) Repeat the fifth and sixth stages of the algorithm K times under high-capacity situations and blind watermarking, and use CAT to extract the watermark.

B. Detecting Scheme

The procedure followed to embed and extract the digital watermark are comparable, but one is the reverse of the other. The three stages of the extraction procedure are the embedding procedure's results, which are the following: firstly, v_{f1} and v_{f2} (i.e., the reference vertices); secondly, M_n (i.e., the fixed-size LCA transition matrix); and finally, the watermarked vector map (see Fig. 9). A detailed overview of the seven steps involved in the extraction procedure is given below.

1) Under the control of the private key, select the reference vertices v_{f1} and v_{f2}, where $1 \le v_{f1}, v_{f2} \le n$, which apply to M's vector map.

2) Calculate the number of vertices in M and the length (N) that will subsequently undergo transformation to produce a domain frequency without the reference vertices.

3) Having collected every feature's set of coordinates, transform into a LCAT transform.

4) Use equation (8) to extract the embedded watermark location, as well as the watermark bits.

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

5) If necessary, apply the third and fourth steps again.

6) Undertake the extraction of the originally embedded watermark W using the private key, which can be achieved by inversing the watermark pattern.

7) Rebuild the watermark pattern to obtain the watermark.

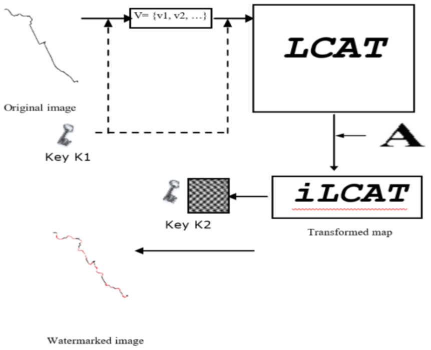


Fig. 8. Embedding Scheme.

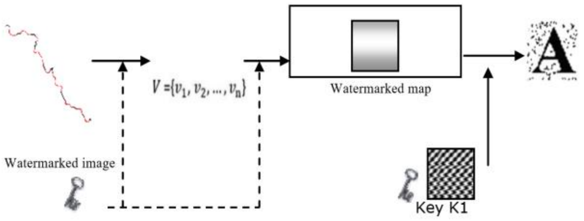


Fig. 9. Detecting Scheme.

C. Evaluation Scheme

The purpose of the evaluation unit is to assess the digital watermarking procedure's quality based on specific indicators. These indicators are listed below, and the purpose of Section VI of this study is to provide an account of the proposed scheme's performance in relation to each indicator (see Fig. 10).

1) Fidelity: Map quality following watermark insertion into the cover work.

2) Robustness: The degree to which the watermarked map is likely to fall under common attacks.

3) Capacity: Watermark coverage.

4) Complexity: The procedure's computational complexity.

5) Security: The degree to which the watermarked zones within the map are secure.

6) Reversibility: An indication of whether a reversibility technique exists that can restore the initial cover work following the extraction of the watermark data.

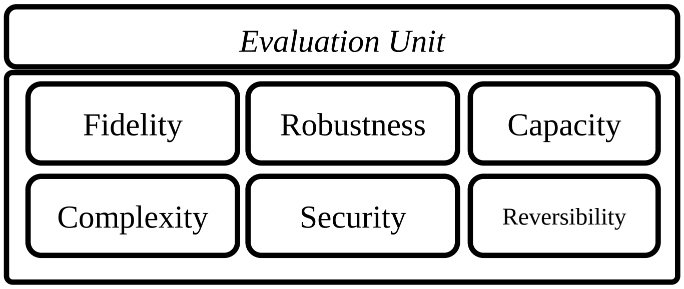


Fig. 10. The Proposed Evaluation Module Watermarked Vector Map Scheme.

VI. Results

The researchers' personal computer was used to conduct the performance evaluation, for which the specifications were as follows: CPU 2.3 GHz, 16GB RAM, Windows 10 Professional, QGIS Version 3.0, Python, and MATLAB. For the data concealing operations, the secret bits associated with every transform coordinate conveyed α in LSB, Mn with a matrix size of 30, and $T = 1$, which indicates iterative embedding. To create the tests, the initial cover work was modified through watermark insertion, and then a range of attacks were levelled against the watermarked vector map (see Fig.11). Following this, the RSME between the watermarked and original maps was computed; the NC between the extracted mark and the original mark was conducted; and finally, the mark was extracted to gauge the level of resistance against attacks.

As indicated in Table I, the proposed scheme was characterised by a high level of resistance against all of the common attacks. In particular, these attacks included Vertex insertion, Vertex deletion (50%), Vertex modification (50%), and the same geometric attacks (namely, rotation, scaling, and translation).

It is worth noting that the proposed scheme was implemented to vector maps. Furthermore, in this case, the map employed represents the Riyadh Development Authority. Additionally, to serve as the watermark, an image was utilised (see Fig. 12). Most importantly, the results of the performance evaluation for the proposed scheme were satisfactory, as shown in Fig. 13 and 14. In particular, Fig. 13 shows that the differences in distance values between the original vector map and the watermarked vector map were not substantial, while Fig. 14 provides an illustration of a well-extracted digital watermark.

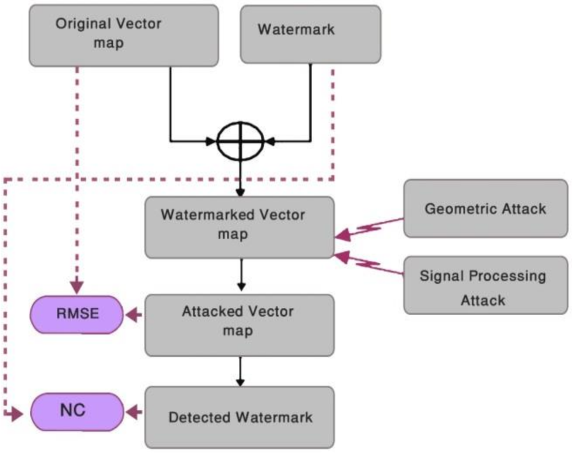


Fig. 11. Test Process.

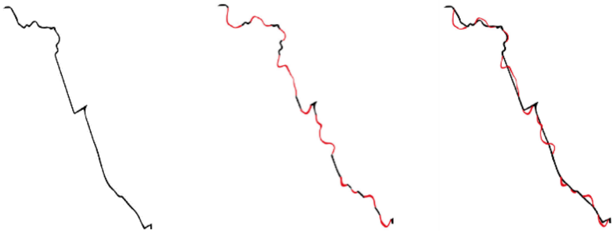
Fig. 12. Example of Watermark.

Further to the results presented in Fig.13, it is clear that the distance values for the vector maps were lower than 0.1 mm, which is critical because this is indicative of the reversibility of the procedure. In other words, the procedure can be considered reversible and, moreover, as having the ability to meet the precision needs of most applications, under a situation where the disparities between the coordinates of the watermarked and original coordinates are not substantial. To improve watermarked vector map's quality, it is necessary to lower distortion by elevating the map's permissible precision tolerance. This is because it lowers the overall number of insertion units, thus lowering the watermark bits' capacity.

The purpose of the evaluation unit was to assess the watermarking system's quality based on the evaluation criteria specified in Section V. D. These evaluation criteria are as follows: namely, fidelity, robustness, capacity, complexity, security, and reversibility. The results of the analysis of each of these evaluation criteria are given in Table II.

TABLE. I. Results of Resistance Facing Different Attack

Deformations	**RMSE between watermarked map and original one (dB)**	**NC between extracted mark and original one (dB)**
Vertex insertion (50%)	0.79	0.76
Vertex deletion ((50%)	0.80	0.76
Vertex modification (50%)	0.82	0.78
Rotation (ρ=60°)	0.94	0.92
Scaling (ς = 0.5)	0.90	0.89
Translation (4.2 , 5.6)	0.91	0.90

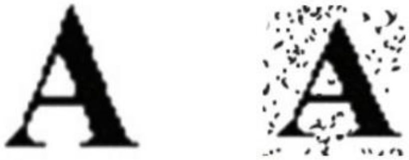


original vector map

watermarked vector map

the difference of them

Fig. 13. Watermark Imperceptivity Proof.



Original Watermark

Extracted Watermark

Fig. 14. Well Extracted Watermark.

TABLE. II. PARAMETERS ANALYSIS OF LCAT

Parameters Analysis	
Evaluation Metrics	LCAT
Invisibility	High
Capacity	High
Reversibly	High
Computational Complexity	Low
Security	High
Geometrical Attacks	83%

VII. CONCLUSION

This study proposed a technique for 2D vector map watermarking using the linear cellular automata transform (LCAT) algorithm. The algorithm is an example of a blind marking algorithm, and it represents a significant contribution in terms of its possible applications in areas such as copyright protection and digital content authentication. Although the performance evaluation yielded positive results, particularly in terms of robustness against attacks, it is important to recognise that the increasingly sophisticated nature of adversaries means that the proposed scheme may not resist every type of attack. That is to say, while the proposed scheme is the product of years of research and expertise in the field of digital watermarking, attackers themselves, as well as the toolkits they have access to, are progressing at the same time. Thus, the authors foresee that the proposed scheme will hold benefits for applications in copyright protection and authentication, but further research should be conducted to devise new methods, and to identify the robustness of the proposed scheme under a broader range of novel and sophisticated attacks.

REFERENCES

[1] Abbas TA, Jawad MJ (2013) Digital vector map watermarking: applications, techniques and attacks Oriental. J Comput Sci Technol 6(3):333–339

[2] Abubahia, A & Cocea, M 2017, 'Advancements in GIS map copyright protection schemes - a critical review', Multimedia Tools and Applications, vol. 76, no. 10, pp. 12205-12231. https://doi.org/10.1007/s11042-016-3441-z.

[3] Abbas T, Jawad M, Sudirman S (2013) Robust watermarking of digital vector maps for copyright protection. In: 14th annual postgraduate symposium on the convergence of telecommunications, networking and broadcasting. 978-1-902560-27-4. Liverpool.

[4] R. Shiba, S. Kang and Y. Aoki: An image watermarking technique using cellular automata transform. In TENCON 2004 IEEE Region 10 Conference (2004), pp. 303–306.

[5] Adwan, A. A. Awwad et al., A novel watermarking scheme based on two dimensional cellular automata, Proc. of the 2011 International Conference on Computers and Computing, pp.88-94, 2011

[6] Blind audio watermarking technique based on two dimensional cellular automata.

[7] AL-ardhi S , Thayananthan V, Basuhail A (2020) Copyright Protection and Content Authentication Based on Linear Cellular Automata Watermarking for 2D Vector Maps. In: Arai K., Kapoor S. (eds) Advances in Computer Vision. CVC 2019. Advances in Intelligent Systems and Computing, vol 943. Springer, Cham.

[8] Lafaye J, B´eguec J, Gross-Amblard D, Ruas A (2007) Geographical database watermarking by polygon elongation. Tech. rep., HAL.

[9] N, Zhang H, Men C (2014) A high capacity reversible data hiding method for 2D vector maps based on virtual coordinates. Comput Aided Des 47:108–117.

[10] Schyndel, R.G., Tirkel, A.Z., Osborne, C.F.: A Digital Watermark. In: ICIP 1994. Proceedings of IEEE International Conference on Image Processing, Austin, USA, vol. 2, pp. 86–90. IEEE, Los Alamitos (1994).

[11] Min LQ, Zhu XZ, Li Q (2012) A robust blind watermarking of vector map. In: Zhang T (ed) Instrumentation, measurement, circuits and systems, advances in intelligent and soft computing, vol 127.Springer, Berlin, pp 51–59.

[12] Wang X, Huang D, Zhang Z (2012) A robust zero-watermarking algorithm for vector digital maps based on statistical characteristics. J Softw 7(10):2349–2356.

[13] Xun W, Hai L, Hujun B (2004) A robust watermarking algorithm for vector digital mapping. J Comput Aided Des Comput Graph 1377–1381.

[14] Niu XM, Shao CY, Wang XT (2007) Gis watermarking: hiding data in 2d vector maps. In: Pan JS, Huang HC, Jain L, Fang WC (eds) Intelligent multimedia data hiding, studies in computational intelligence, vol 58. Springer, Berlin, pp 123–155.

[15] Wang N, Men C (2012) Reversible fragile watermarking for 2-d vector map authentication with ocalization. Comput Aided Des 44(4):320–330.

[16] Wang N, Men C (2013) Reversible fragile watermarking for locating tampered blocks in 2d vector maps. Multimedia Tools Appl 67(3):709–739.

[17] Mouhamed M, Rashad AM, ella Hassanien A (2012) Blind 2d vector data watermarking approach using random table and polar coordinates. In: 2nd international conference on uncertainty reasoning and knowledge engineering, pp 67–70.

[18] Li A, Lin BX, Chen Y, Lu G (2008) Study on copyright authentication of gis vector data based on zero-watermarking. Int Arch Photogramm Remote Sens Spat Inf Sci 37:1783–178.

[19] Cao L, Men C, Li X (2010) Iterative embedding-based reversible watermarking for 2d-vector maps. In:17th IEEE international conference on image processing, pp 3685–3688.

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

[21] Ling Y, Lin CF, Zhang ZY (2012) A zero-watermarking algorithm for digital map based on dwt domain. In: He X, Hua E, Lin Y, Liu X (eds) Computer, informatics, cybernetics and applications, LNEE, vol 107. Springer, Netherlands, pp 513–521.

[22] Neyman SN, Pradnyana INP, Sitohang B (2014) A new copyright protection for vector map using fft based watermarking. TELKOMNIKA Telecommunication, Computing. Electron Control 12(2):367– 37.

[23] Martı and G. Rodrı: Reversibility of linear cellular automata. Applied Mathematics and Computation 217 (21) (2011), 8360–8366

[24] S. Wolfram, Theory and Applications of Cellular Automata, World Scientific Publishing Company, Singapore, 1986.

[25] S. Wolfram, Cryptography with Cellular Automata, Springer- Verlag, Beilin, 1986.