American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-12, pp-404-409
www.ajer.org
Research Paper Open Access

A New Digital Watermarking Scheme of Content Authentication of Vector Maps

Mohammed W. Abo A[1]_Soud[1], LoaiKayed B.Melhim[2]
[1](Department of Computer Science and Information, College of Science/ MajmaahUniversity, Zulfi, Saudi Arabia)
[1](Department of Information Systems, College of Computers and Informatics / Suez CanalUniversity, Ismailia)
[2](Department of Computer Science and Information, College of Science/ MajmaahUniversity, Zulfi, Saudi Arabia)
Corresponding Author: Mohammed W. Abo A[1]

ABSTRACT: *For 2-D vector maps, reversible fragile watermarking is mainly used to protect the integrity and authenticity content of the data. The proposed scheme in this research is introduced in two stages. The first stage will explain how to extract the vector map characteristics embeds them and marks the location of each spatial feature, divides the features of a vector map into blocks; these blocks are then divided into non over-lapped equal segments. The integrity watermark for each block is divided into two parts: content authentication and zooming authentication. The zooming authentication is performed by identifying any 2D scaling attempt. The scaling attempt is detected by using the calculated area of a planar non-self-intersecting polygon with arrays of the x and y coordinates of the vertices, traced in a clockwise direction. The second stage in the presented model will explain how to identify and locate tampered features and tampered regions. After this part is completed, it will be integrated other components to establish the complete Digital Watermarking Scheme for Vector Maps.*

Keywords: *Content authentication, Features, Integrity, Reversible fragile, Vector map, Zooming authentication*.

Date of Submission: 20-12-2017 Date of acceptance: 03-01-2018

I. INTRODUCTION

Computer communication and the Internet development makes it very difficult to protect the digital media such copyright protection, hiding communication, data authentication, data tracing (fingerprinter), etc. Watermarking has been introduced as a possible solution for these issues. In watermarking cover data could be any of digital data types, e.g. digital image, audio, video, text, bar-code, 3D model, CAD data, 2D vector data, soft wares, VLSI, etc. Among these data types, different multimedia data such as digital images, audios, videos and 3D models have got more interest than other data types[1-8].

This paper focuses on watermarking 2D digital vector maps, which are considered a valuable part of Geographical Information System (GIS). 2-D vector maps have been intensively used in many military and civil applications. Although the acquisition of these vector geo-spatial data is a high-cost process [9, 10], online available tools and equipment, makes the process of maliciously modifying these valuable data, an easy work. Tools that verify and ensure the integrity of the 2-D vector map content are needed. The integrity of 2-D vector map refers to the authenticity of the 2-D vector map data, that is, whether the 2-D vector map data has been manipulated with a common or malicious data. Different watermarking technologies can be used to embed hidden information in a digital map in order to indicate the author and to authenticate the integrity of the contents[1, 11]. In reversible watermarking, full extraction of the embedded information along with the complete restoration of the original form is available[2, 8, 12-14]. Fragile watermarking is mainly used to protect the integrity and authenticity content of the data [15]. Once tampered with any kind of modification the watermark breaks. Therefore, a fragile watermarking that exploits reversible watermarking schemes to embed the authentication data cannot only locate malicious attacks but also recover the original content[13]. Thus 2D vector map integrity and authenticity can be guaranteed through the use of fragile watermarking techniques.Watermarking has been used as copyright protection [16-19]and tamper detection [3, 4, 15]in 2D

vector maps. Watermarking implies that the content is distorted in an irreversible way; the nature of vector maps does not desire such modifications. Therefore, reversible fragile watermarking schemes are greatly needed.

While Many researches have been carried out on reversible fragile watermarking for different digital types [6-8]; little researches have been performed on 2D vector map e.g. [2-5]. To the best of our knowledge no researches have been proposed for the map zooming attack in 2D vector maps. Map zooming refers to altering the size of the map in all axes, axes altering will change the distances between the vector map points, this change can be increasing i.e. zoom in or decreasing zoom out[20]. This paper will adopt the technique presented by [3, 4] to cover the embedding and extraction of the watermark and will address the problem of map zooming for 2D vector maps.

II. RELATED WORK

A new hybrid, secure and robust image watermarking scheme based on the IWT and SVD is proposed. This scheme utilizes the properties of IWT and SVD transforms to achieve the watermarking requirements. These properties include the good stability of the SVD and the ability of the IWT to preserve a perfect reconstruction, in which integers are mapped to integers. In addition to the blind issue, the security is improved and guaranteed by including a digital signature authentication mechanism. The digital signature authentication mechanism helps to solve the false positive problem which is one of the important problems in the watermarking area [MK2014]. A 2-D vector map is very important data in the surveying and mapping fields. It is considered to be content for which verification of integrity and authenticity are urgently required. Using a novel marking technique and a reversible data-hiding method, this scheme detects and locates malicious attacks with high accuracy while ensuring exact recovery of the original content [21].

The scheme presents a 2D vector graphics watermarking algorithm based on foundational contour. This algorithm by reducing the changes of the main body information and removing the extracted foundational contour in the transform domain embeds the watermarks, so as to achieve a more robust watermarking embedding effect[22]. Digital watermarking has been used for a long time in digital media, such as the information used in geographic information system (GIS) and digital vector maps, for both authentication and tracing. This work proposes a digital watermarking algorithm for vector map, which based on data configuration of vector map, combines with the theory of error correction in the field of digital communication. The theoretic analysis and experimental results show that the algorithm make the embedded watermarking induces loss distortion, and it can resist some common manipulations[23]. Among the newly explored research areas of digital watermarking, various types of data embedding technologies for vector graphics have drawn more and more attention. The features of vector graphics on the data expression and use were analyzed. The requirements of watermarking were discussed [24]. Digital watermarking Algorithm is composed of three parts: watermark embedding algorithm, the watermark extraction algorithm and the watermark detection algorithm [25]. This paper proposes a digital watermarking for vector maps, some significant character strings can be embedded into vector maps. Theoretic analysis and experimental results show that, the embedded watermarking induces less distortion, and it can resist some common manipulations, such as translation, rotation, scaling, vertex insertion/removal and local modification attacks, namely, it has perfectible robustness [26]. Visually recognizable watermarks can add extra information like integrity and authentication, while blind watermarks do not need the original data to be published for the detection. This work presents a semi-blind version of RAW Vec, i.e. a method that uses the original vector map during the detection without revealing it, but maintains the watermark as a raster image [27].

An invisible watermarking scheme based on polylines and polygons for the copyright protection of a GIS digital map[28]. The scheme clusters all polylines and polygons in the feature layers of the map on the basis of the polyline length and the polygon area. And then a watermark is embedded in GIS vector data on the basis of the distribution of polyline length and polygon area in each group by moving all vertices in polylines and polygons within a specified tolerance. Experimental results confirm that the scheme is more robust against geometric attacks, such as rotation, scaling, and translation (RST) transformations, data addition, cropping, breaking, and filleting attacks, and layer attacks with rearrangement and cropping, when compared with conventional schemes. This research paper introduces a prototype for Digital Image Authentication System (DIAS). This system can perform visible and invisible watermarking on image. DIAS is applicable for color and gray images. The input image could be of any size, and the resultant image size would be same as input image. DIAS identifies the ownership of digital image using Digital Watermarking.

The Digital watermarking concept is used to hide and detect information from image. It is the best way to copyright protection of the user. By the use of digital watermarking, user can blame on faker for ownership. This is known as an Authentication System for ownership identification [29]. The main concern of digital watermarking is to prove ownership as well as protection of the embedding information. This paper gives brief

overview of existing audio watermarking techniques, their applications and future prospects of digital watermarking [30].

III. REVERSIBLE DATA HIDING SCHEME

The features of the vector map are first divided into blocks; each of these blocks contains the same area. Suppose $X = \{x_i | i \in [1, n]\}$ is an x coordinate list composed of n elements, x_{st} is the starting point of coordinate X and x_{fi} is the end point of coordinate X. The length of each segment l_t is calculated by

$$\boldsymbol{l_t = (x_{fi} - x_{st})/D_x} \quad \textbf{(1)}$$

Then the distance between x_{st} and x_{fi} is divided into $D_x (D_x \geq 2)$equal segments. After that, a position of two coordinates x_{max} and x_{min} are calculatedfor each segment D_{xi}; and $i = \{1,2, \dots, D_{x-1}\}$, where x_{max} and x_{min} are the maximum and the minimum coordinates of D_{xi}, and an interval $a_{D_{xi}} (x_{min}, x_{max})$ is formed for each segment D_{xi}. Then A_{D_x} is defined as

$$\mathbf{A_{D_x} = \{a_{D_{xi}} | i \in [1, D_{x-1}]\}} \quad (2)$$

A_{D_x} represents the all calculated x_{max} and x_{min} for D_x segments.

Then, $\mathbf{A_{D_x} = \{(x_{min}^{Dx1}, x_{max}^{Dx1}), (x_{min}^{Dx2}, x_{max}^{Dx2}), \dots, (x_{min}^{Dxi-1}, x_{max}^{Dxi-1})\}; x_{max}^{i-1} \leq x_{min}^{i}}$

Similarly the same calculations will be performed for the Y coordinates to produce interval $\mathbf{a_{D_{yi}}(y_{min}, y_{max})}$ for each segment D_{yi}. Then A_{D_y} is defined as

$$\boldsymbol{A_{D_y} = \{a_{D_{yi}} | i \in [1, D_{y-1}]\}} \quad (3)$$

A_{D_y} represents all the calculated y_{max} and y_{min} for D_y segments.

Then.$\boldsymbol{A_{D_y} = \{(y_{min}^{Dy1}, y_{max}^{Dy1}), (y_{min}^{Dy2}, y_{max}^{Dy2}), \dots, (y_{min}^{Dyi-1}, y_{max}^{Dyi-1})\}}$

Next, define the vector A_{fr} by the following equations:

$$\boldsymbol{A_{fr1} = \left| \frac{(x_{max}^{Dx1} \times y_{max}^{Dy1}) - (x_{min}^{Dx1} \times y_{min}^{Dy1})}{2} \right|}$$

$$\boldsymbol{A_{fr2} = \left| \frac{(x_{max}^{Dx2} \times y_{max}^{Dy2}) - (x_{min}^{Dx2} \times y_{min}^{Dy2})}{2} \right|}$$

$$\boldsymbol{A_{fri} = \left| \frac{(x_{max}^{Dxi} \times y_{max}^{Dyi}) - (x_{min}^{Dxi} \times y_{min}^{Dyi})}{2} \right|}$$

$$A_{fr} = \{A_{fri} | i \in [1, D_{x-1}]\} \quad (4)$$

The vector A_{fr} represents the calculated areas for all D_x segments in one feature. In the following Fig.1, an example of the areas for D_x segments for one feature into the group. The final step will to calculate A_{fr} for the rest of the features in the group, the resulted A_{fr} will be grouped in a vector called A_{gr}.

$A_{gr} = \{A_{frj} | j \in [1, N]\}$, whereN is the number of features in a group. (5)

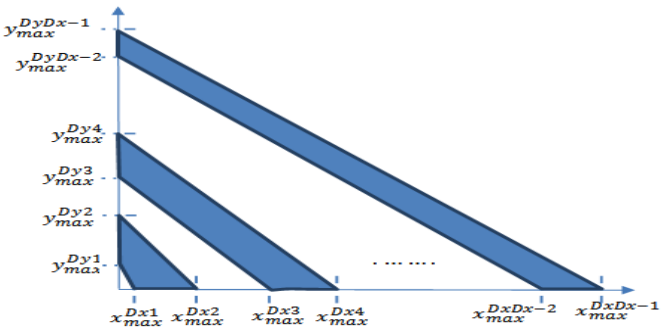

Fig. 1 An Example of the areas for D_x segments for one feature into the group

IV. AUTHENTICATION WATERMARK GENERATION

For different types of blocks, different A_{gr} values will be calculated, these calculated values for every block B_i will be called $A_{gr}(B_i)$. Assuming the generated authentication watermark is given by H_i and H_i^s for any block B_i.

$$H_i = \text{blockhash}(\text{hash}(I(B_i), k, i, M_i), L, K) \quad \ldots\ldots\ldots \text{32 bit} \tag{6}$$

$$H_i^s = \text{blockhash}\left(\text{hash}\left(k, i, A_{gr}(B_i)\right), L, K\right) \quad \ldots\ldots\ldots \text{32 bit} \tag{7}$$

$$W_i(64\text{ bit}) = H_i(32\text{ bit})H_i^s(32\text{ bit}) \tag{8}$$

Where I(.) is the method for acquiring the spatial data and attribution data of all features in B_i, k is a private key to generate a random number for the input of hash(.), M_i denotes the vector map index, $A_{gr}(B_i)$ is a vector represents the calculated areas of the features in the contained group in block B_i , hash(.) represents an existing cryptographic hash method, L is the length of the generated watermark bits *blockhash(R1,L,K)*, *blockhash(R2,L,K)* are functions return L bits from stringsR1,R2 in a random fashion under the control of a private key K, and the bit string H_i, $\mathbf{H_i^s} = \{\mathbf{h_{i,j}} | \mathbf{h_{i,j}} \in \{\mathbf{0}, \mathbf{1}\}, \mathbf{j} \in [\mathbf{0}, \mathbf{L-1}]\}$ of length L is the generated watermark.The watermark $W_i(64\text{ bit})$ is generated by equations (6), (7) and (8). Then W_i will be embedded in the block B_i into the vector map using Wang et.al method (REF). The addition of the water mark W_i will generate a new block vector B_i'.

V. AUTHENTICATION WATERMARK VERIFICATION

The following steps show how to verify each block's integrity and recover its original size. Firstly, the features of the embedded vector map M' will be divided into non-overlapped blocks. Then, extract the watermark W_i' using Wang et al.'s reversible watermarking method. After that, a watermark is derived from the recovered content with the watermark generation function W_i. A tampered block can be detected by the mismatch between W_i' and W_i. A block is considered authentic if the two watermarks are equal, otherwise it is seen as tampered (contents modification or map zooming (in / out).

For tampered blocks, consider the last 32 bit of the derived watermark W_i which was called H_i^s and the last 32 bit of the extracted watermark W_i' and will be known as $H_i^{s'}$. The next step is to match between H_i^s and $H_i^{s'}$; a mismatch indicates a zoom in/out modification has been performed, otherwise only the contents were tampered; for tampered contents, Wang et.al will be applied. In case of zoom in/out equation (7) will be used with H_i^s and $H_i^{s'}$ to derive $A_{gr}(B_i)$ and $A_{gr}'(B_i)$. The derived $A_{gr}{}'(B_i)$ include all the features in a watermarked block, $\mathbf{A'_{gr}} = \{\mathbf{A'_{frj}} | \mathbf{j} \in [\mathbf{1}, \mathbf{N}]\}$. For all j values compare A'_{frj} with A_{frj} to determine which j features have been zoomed.

$$\begin{cases} A_{frj} - A'_{frj} = 0, \text{no zooming} \\ A_{frj} - A'_{frj} > 0, zoom\ out \\ A_{frj} - A'_{frj} < 0, zoom\ in \end{cases} \tag{9}$$

To locate the modified segment, use equation 4 to calculate A'_{fri}, a comparison with A_{fri} will locate D_{xi} as shown in Fig. 2. The last step after locating the modified segment is to specify the zooming percentage S , which is given by

$$S = \frac{A'_{fri}}{A_{fri}} \times 100\% \tag{10}$$

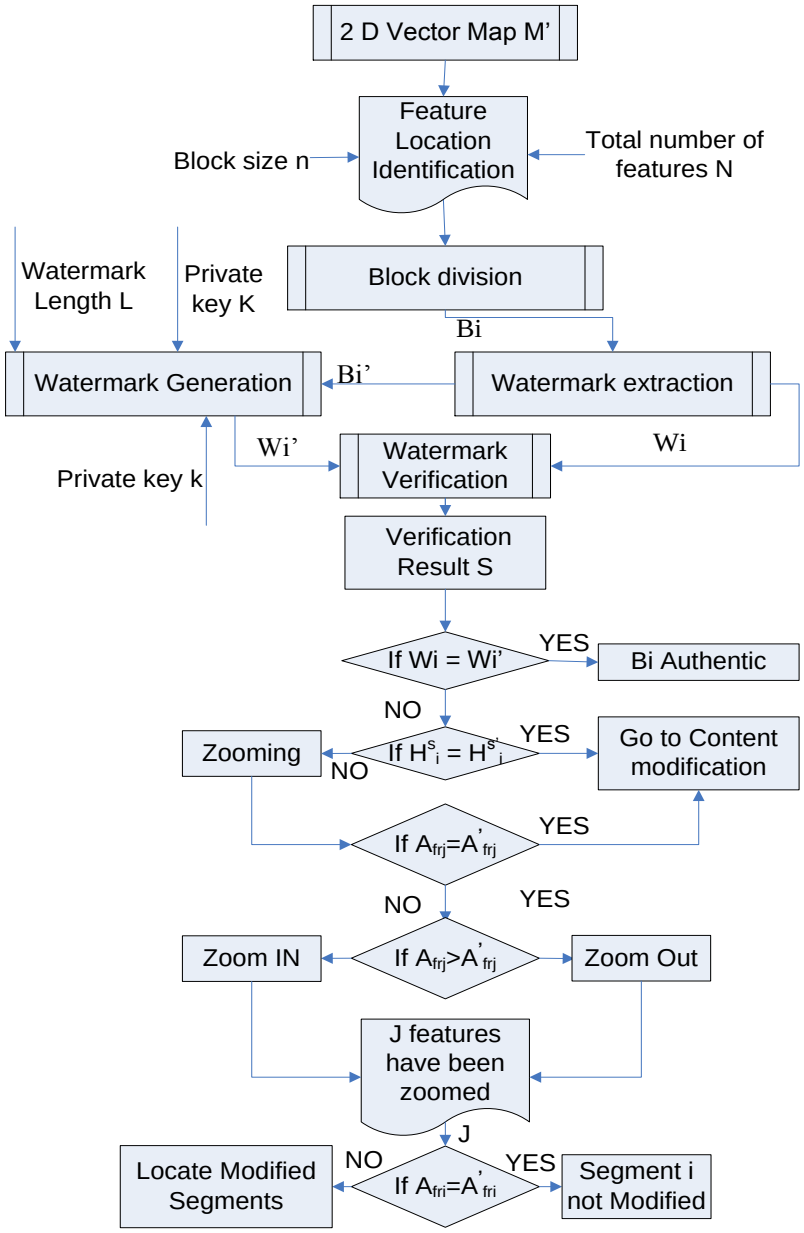

Fig. 2 Watermark Verification

VI. CONCLUSION

2D digital vector maps, which are considered a valuable part of Geographical Information System (GIS), have been intensively used in many military and civil applications. Although the acquisition of these vector geo-spatial data is a highly cost process, online available tools and equipment, make the process of maliciously modifying these valuable data, an easy work. Protection of these valuable resources is a must. The proposed approach presented an authentication model that can detect any malicious zooming in/out and specify the zooming percentage for the 2D digital vector maps.

ACKNOWLEDGEMENTS

The authors would like to thank the deanship of scientific researchand Research Center for engineering and applied sciences, Majmaah University, Saudi Arabia, for their support and encouragement; also the authors would like express our deep thanks to our College (College of Science at Zulfi City, Majmaah University, Saudi Arabia).

REFERENCES

[1]. L. Cao, C. Men, and Y. Gao, "A recursive embedding algorithm towards lossless 2D vector map watermarking," Digital Signal Processing, vol. 23, pp. 912-918, 2013.

[2]. S. N. Neyman, B. Sitohang, and S. Sutisna, "Reversible fragile watermarking based on difference expansion using manhattan distances for 2d vector map," Procedia Technology, vol. 11, pp. 614-620, 2013.
[3]. N. Wang and C. Men, "Reversible fragile watermarking for 2-D vector map authentication with localization," Computer-Aided Design, vol. 44, pp. 320-330, 2012.
[4]. N. Wang and C. Men, "Reversible fragile watermarking for locating tampered blocks in 2D vector maps," Multimedia tools and applications, vol. 67, pp. 709-739, 2013.
[5]. N. Wang, H. Zhang, and C. Men, "A high capacity reversible data hiding method for 2D vector maps based on virtual coordinates," Computer-Aided Design, vol. 47, pp. 108-117, 2014.
[6]. M. Arsalan, S. A. Malik, and A. Khan, "Intelligent reversible watermarking in integer wavelet domain for medical images," Journal of Systems and Software, vol. 85, pp. 883-894, 2012.
[7]. H.-T. Chan, W.-J. Hwang, and C.-J. Cheng, "Digital hologram authentication using a hadamard-based reversible fragile watermarking algorithm," Journal of Display Technology, vol. 11, pp. 193-203, 2015.
[8]. J.-N. Chang and H.-C. Wu, "Reversible fragile database watermarking technology using difference expansion based on svr prediction," in Computer, Consumer and Control (IS3C), 2012 International Symposium on, 2012, pp. 690-693.
[9]. A. Carrara, F. Guzzetti, M. Cardinali, and P. Reichenbach, "Use of GIS technology in the prediction and monitoring of landslide hazard," Natural hazards, vol. 20, pp. 117-135, 1999.
[10]. L. Montoya, "Geo-data acquisition through mobile GIS and digital video: an urban disaster management perspective," Environmental Modelling & Software, vol. 18, pp. 869-876, 2003.
[11]. P. Singh and R. Chadha, "A survey of digital watermarking techniques, applications and attacks," International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, pp. 165-175, 2013.
[12]. Z.-x. Lin, F. Peng, and M. Long, "A reversible watermarking for authenticating 2D vector graphics based on bionic spider web," Signal Processing: Image Communication, 2017.
[13]. F. Peng, Z.-J. Yan, and M. Long, "A Reversible Watermarking for 2D Vector Map Based on Triple Differences Expansion and Reversible Contrast Mapping," in International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, 2017, pp. 147-158.
[14]. N. Wang and X. Zhao, "2D vector map data hiding with directional relations preservation between points," AEU-International Journal of Electronics and Communications, vol. 71, pp. 118-124, 2017.
[15]. H. Lan and Y. Peng, "Reversible Fragile Watermarking for Fine-Grained Tamper Localization in Spatial Data," in Australasian Database Conference, 2017, pp. 233-247.
[16]. B. Surekha and G. Swamy, "Sensitive Digital Image Watermarking for Copyright Protection," IJ Network Security, vol. 15, pp. 113-121, 2013.
[17]. R. Saxena, K. Shah, R. Chawla, and V. Santhi, "Biometric Watermarking for Copyright Protection of Digital Images," International Journal of Applied Engineering Research, vol. 9, pp. 23681-23688, 2014.
[18]. B. Wang, J. Su, Y. Zhang, B. Wang, J. Shen, Q. Ding, et al., "A Copyright Protection Method for Wireless Sensor Networks Based on Digital Watermarking," International Journal of Hybrid Information Technology, vol. 8, pp. 257-268, 2015.
[19]. T. K. Tewari, "Novel Techniques for Improving the Performance of Digital Audio Watermarking for Copyright Protection," 2015.
[20]. J. Zdravkovic, M. Kirikova, and P. Johannesson, Advanced Information Systems Engineering: 27th International Conference, CAiSE 2015, Stockholm, Sweden, June 8-12, 2015, Proceedings vol. 9097: Springer, 2015.
[21]. N. M. Makbol and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," Digital Signal Processing, vol. 33, pp. 134-147, 2014.
[22]. Z. Junfeng and X. Bing, "Research on digital watermarking algorithms for 2d graphics," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, 2011, pp. 179-183.
[23]. F.-j. Cheng, H. Yin, X.-p. Zhang, and D.-x. Zhang, "A digital watermarking algorithm for vector map," in Challenges in Environmental Science and Computer Engineering (CESCE), 2010 International Conference on, 2010, pp. 101-103.
[24]. L. Zheng, R. Chen, L. Li, and Y. Li, "Study on digital watermarking for vector graphics," in Education Technology and Computer Science (ETCS), 2010 Second International Workshop on, 2010, pp. 535-538.
[25]. Y. Zhang, "Digital watermarking technology: A review," in Future Computer and Communication, 2009. FCC'09. International Conference on, 2009, pp. 250-252.
[26]. C. Zhang, X. Zhang, D. Zhang, and Y. Jiao, "Digital watermarking of vector map based on vector angle," in Intelligent Computation Technology and Automation (ICICTA), 2008 International Conference on, 2008, pp. 127-130.
[27]. K. Magalhaes and R. Dahab, "Sb-rawvec-a semi-blind watermarking method for vector maps," in Communications, 2009. ICC'09. IEEE International Conference on, 2009, pp. 1-6.
[28]. S.-H. Lee and K.-R. Kwon, "Vector watermarking scheme for GIS vector map management," Multimedia tools and applications, vol. 63, pp. 757-790, 2013.
[29]. N. Bhargava, M. Sharma, A. S. Garhwal, and M. Mathuria, "Digital image authentication system based on digital watermarking," in Radar, Communication and Computing (ICRCC), 2012 International Conference on, 2012, pp. 185-189.
[30]. S. P. S. Chauhan and S. Rizvi, "A survey: Digital audio watermarking techniques and applications," in Computer and Communication Technology (ICCCT), 2013 4th International Conference on, 2013, pp. 185-192.

Mohammed W. Abo A "A New Digital Watermarking Scheme of Content Authentication of Vector Maps." American Journal of Engineering Research (AJER), vol. 6, no. 12, 2017, pp. 404-409.