Proposed an Intelligent Watermarking in GIS Environment

Tawfiq A. Abbas[1], Majid J.Jawad[2]

[1]College of Information Technology, Babylon University, Iraq

[2]College of Science, Computer Science Dept., Babylon University, Iraq

[1]tawfiqasadi63@yahoo.com; [2]majid_al_sirafi@yahoo.com

***Abstract*- GIS (Geographic Information System) has been used in military and commercial applications for many years. The data of GIS are very expensive. So, it is very important to prevent any illegal use of these data. Digital watermarking can provide potential solution. As we know, in most of the applications of digital watermarking, the watermark is used to protect the copyright of digital product. In the other word, the product (cover) is important. According to this fact, we presented 2D vector map watermarking for GIS digital map based on a new watermarking concept called intelligent watermarking. The need of this concept is increased in the last years to protect the wide range of digital maps data transmitted via computer networks. Briefly, the scheme depends on the feature of the cover. The embedding of the watermark can be done in several steps. First extracting some features from the original digital vector map. Second combine these features with external watermark in order to get the intelligent watermark. Third embed the intelligent watermark in the vector map to get the watermarked vector map. The extracting of the watermark can be done in several steps. First, extract the intelligent watermark from the watermarked digital vector map. Second decompose the intelligent watermark into features and external watermark. Third reverse the extracted features to features of watermarked vector map. So, if the watermarked vector map is attacked, this watermarked vector map will be distorted, otherwise will not be distorted. Our proposed scheme can be applied in all the other media.**

Keywords*- *Intelligent Watermark; Copyright Protection; GIS; Digital Vector Map

I. INTRODUCTION

GIS has been used in military and commercial applications for many years. The main component of GIS is the data. The GIS data has two important properties. First, the effort it takes to put it in a form suitable for use in the GIS applications. This effort increases its cost. Second, in most cases the GIS Data contains confidential information which must be kept away from unauthorized users. Such confidential information includes GIS layers containing troop locations and additional information like movements and mines places in a tactical environment. So, it is very important to protect the GIS data from two threats. First, since the GIS data is too expensive, it is very important to prevent illegal duplication and distribution of it. Today, it is too easy for a company to buy some GIS layers, make illegal copies from them and distribute or sell them many times without taking any permission from the original GIS data provider. Second, since the GIS data is sensitive and must not be accessed by unauthorized users, it is very important to enforce some kinds of access control on it [10].There are several technologies having been used such as cryptography, but this technology doesn’t provide efficient solution. Digital watermarking technology can provide efficient solution to the above crucial problem. In general, digital watermarking means digitally adding a small amount of data (referred to as watermark) in a digital object (host). The information encoded in the watermark can be used to identify the copyright owner of the object or to detect any tampering performed onto the object**.** Digital watermarking can be used in several applications such as copyright protection, fingerprinting, tamper proofing, broadcast monitoring, etc. There are several cases in which digital watermarking technology can be classified, such as according to the extraction of watermark where in this case the watermarking can be blind or non-blind. In blind the original cover is not needed, while in non-blind the cover is needed. Another classification depends on the space in which the watermark is embedded, where there are two spaces, spatial domain and frequency domain. In spatial domain, the watermark is embedded directly in the data, while in frequency domain, the watermark is embedded in the coefficient of the data. Digital watermarking needs several requirements;*first*, Perceptual transparency, in which, the inserted watermark should not affect the quality of the cover media; *second*, robustness, which means the measure of the ability of the embedding algorithm to introduce the watermark in such a way that it is retained in the source content despite several stages of processing; *third*, security of a watermarking technique which can be judged the same way as with an encryption technique; *fourth*, pay load of watermark which means, the amount of bits that the watermark signal carries depends on the application, reversibility, which means restoring the original cover after extracting the watermark [8, 6]. Digital watermarking can be applied in several media, such as image, video, audio, text, 2D and 3D vector map [5, 2, 3, 1, 4, 7].

The rest of the paper is organized as follows. In Section 2, the differences between the intelligent watermarking and fragile watermarking are listed. In Section 3, proposed algorithm is presented .Experimental results and capability analyses are shown in Section 4. Conclusions and future works are drawn in Section 5.

II. DIFFERENCES BETWEEN INTELLIGENT WATERMARKING AND FRAGILE WATERMARKING

There are several differences between intelligent watermarking and fragile watermarking

1. In intelligent watermarking, the attacker can't benefit the cover (product) (after attacking it), since the cover will be distorted, while in fragile watermarking the attacker can benefit the cover (product).

2. The goal of the fragile watermarking is to detect any tampering in the cover, while the goal of the intelligent watermarking can be used in the following applications:

- Detecting any tampering in the cover (fragile watermarking);
- Detecting and correcting any tampering in the cover (semi fragile watermarking);
- Copyright protection of the cover (robust watermarking).

III. PROPOSED SCHEME

In most of the applications of digital watermarking, the watermark is used to protect the copyright of digital product. The attacker of watermark aims to remove the watermark or prevent the extraction of it. So, in this case, the owner cannot prove whether the product is his or not. So, later, the attacker can benefit from this product. In the other meaning, in the watermarking applications, the cover is important. The proposed watermarking algorithm is designed to distort the cover when it is attacked. This distortion is done by using intelligent watermark. The proposed method consists of two stages.

A. Embedding the Watermark

This stage can be listed in the following steps:

1) Extracting the features from the cover, this satisfies the intelligent aspect in watermarking, such as texture, pixels, etc. in image or coordinates in vector map.

2) Composing the extracted features with given external watermark (traditional watermark) in order to get the intelligent watermark by using Formula 1 below:

$$Iw = comp\ (ewm, f) \tag{1}$$

Where ***iw***, ***comp***, ***ewm, and f*** is the intelligent watermark, the composition function, the external watermark, and the extracted features, respectively.

3) Embedding the intelligent watermark in the cover and get the watermarked cover.

Fig. 1 shows the embedding procedure.

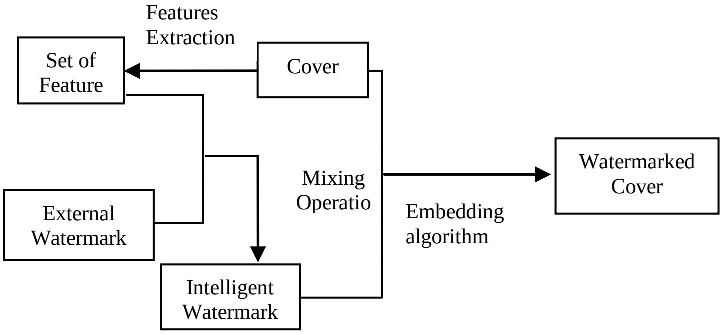


Fig. 1 Embedding watermark Operation

B. Extracting the Watermark

This stage can be listed in the following steps:

1) Extracting the intelligent watermark (which contains the traditional watermark and the features) from the watermarked cover.

2) Decomposing the extracted intelligent watermark into features and traditional watermark by using Formula 2 below:

$$(ewm, f\,) = decom\ (eiwm) \tag{2}$$

Where ***ewm***, ***f, decom, eiwm***are the external watermark, and the features, the decomposition function, the extracted intelligent watermark, respectively.

3) Reflecting the extracted features (which are selected after decomposition operation) on the features of watermarked media. So, if the features of watermarked cover are equal to the extracted features, this reflection won't distort the watermarked cover (that's means there is no attacking on the watermarked cover), but if the features of watermarked cover is not equal to the extracted features, this reflecting will distort the watermarked cover (that's means there is attacking on the watermarked cover) and the attacker won't benefit the watermarked cover.

Fig. 2 shows the extracting and verification procedure.

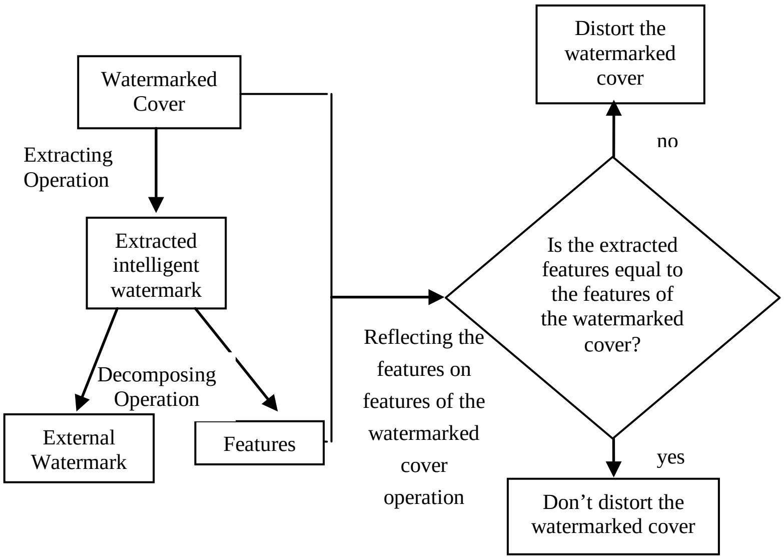

Watermarked Cover
Extracting Operation
Extracted intelligent watermark
Decomposing Operation
External Watermark
Features
Reflecting the features on features of the watermarked cover operation
Is the extracted features equal to the features of the watermarked cover?
no
Distort the watermarked cover
yes
Don't distort the watermarked cover

Fig.2 Extracting and verification operation

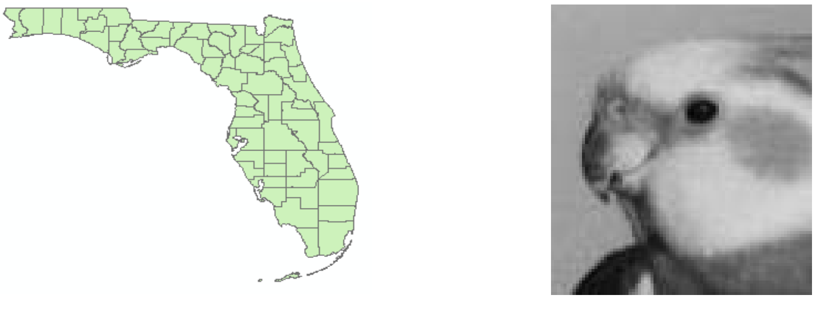
IV. EXPERIMENTAL RESULTS

A. The background of the Vector Map

The data of GIS are stored in two forms raster and vector. Since we took the vector map as a case study of our proposed scheme, let us show, briefly, some information about the vector map. Vector map data are normally composed of spatial data, attribution data, and some additional data are used as indices or extra descriptions, etc. Spatial data describe the geographical locations of the map objects which represent the geographical objects in the real world and always take the form of three basic geometrical elements, i.e. points, polylines and polygons. All these map objects are formed by many organized vertices. Spatial data are actually a sequence of coordinates of these vertices based on a certain geographical coordinate system. Attribution data describe the properties of map objects such as their names, categories and some other information. It is obvious that the information recorded by attribution data is very important and cannot be modified arbitrarily, so does the other additional data mentioned above. In all proposed watermarking algorithms, the space for embedding watermark is provided by the spatial data, i.e. the coordinates of vertices [9].

B. Choosing the Watermark and the Cover

To evaluate the scheme, 2-D vector map (as a cover) is used. Also, the image of size 70x90 pixels is used as external watermark. Fig. 3 shows original vector map and external watermark.



(a) (b)

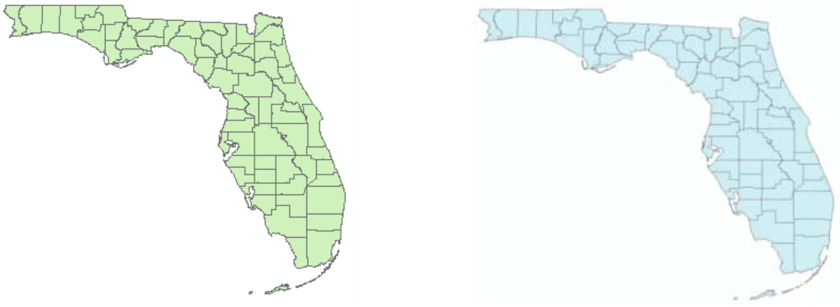
Fig.3 (a) Original vector Map (b) Original Watermark

C. Preparing the Intelligent Watermark

The preparing of the intelligent watermark can be done firstly, by extracting some features from the cover. In this case we extracted the any bit of integer part of the selected coordinates from the map (for example we used the fourth bits). Secondly these extracted features are composed with the external (original) watermark, by using Formula 1

D. Embedding the Intelligent watermark

After preparing the intelligent watermark, we embedded it by using least significant bit technique (we can use any embedding technique).Fig. 4 shows the original vector map and watermarked vector map.

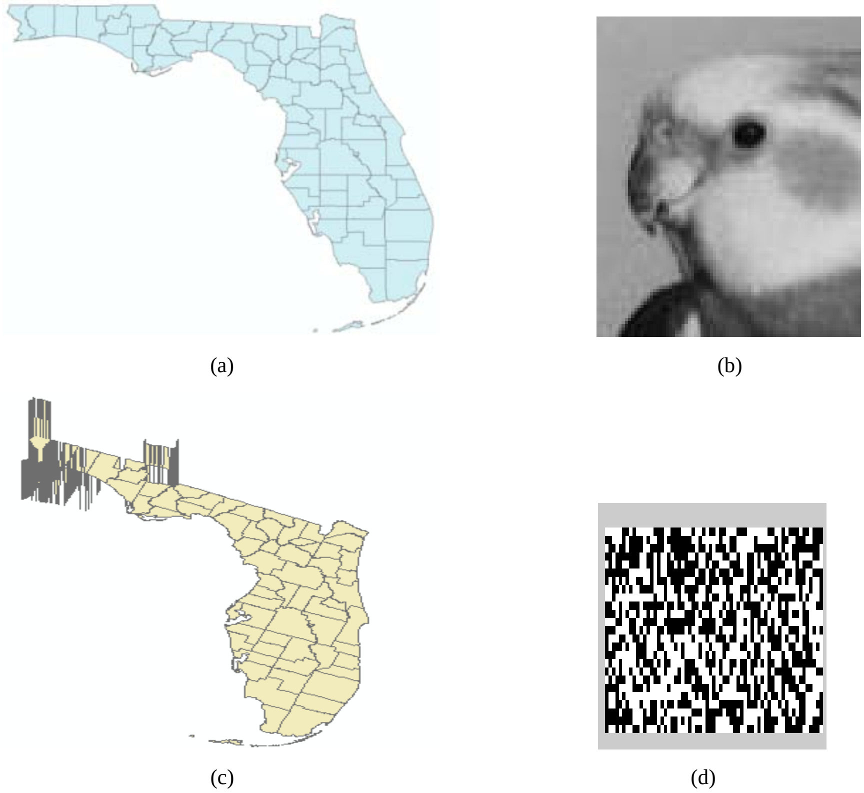


(a) (b)

Fig.4 (a) Original Map (b) Watermarked map

E. Extracting the Watermark

The extracting watermark can be done firstly by extracting the intelligent watermark: secondly decomposing the intelligent watermark into features (selected bits of the coordinates) from the extracted intelligent watermark by using Formula 2: thirdly, reflecting the features (bits) on the fourth bits of the coordinates of the watermarked vector map. So, if no attack this means that the extracted feature (bits) is equal to the fourth bits of the coordinates of the watermarked vector map and the map doesn't distorted, but if the watermarked vector map is attacked, the extracted feature (bits) is not equal to the fourth bits of the coordinates of the watermarked vector map and the map is distorted. Fig. 5 shows the not attacked watermarked vector map, attacked watermarked vector map, extracted watermark without attacking, extracting watermark with attacking.



(a) (b)

(c) (d)

Fig.5(a) verified watermarked vector map without attacking (b) extracted watermark without attacking
(c)verified watermarked vector map with attacking (rotation attack) (d) extracted watermark after attacking (rotation attack)

V. CONCLUSIONS AND FUTURE WORKS

In this paper, we introduced a new trend in information hiding by proposing a novel algorithm. In this algorithm, we convert the traditional watermark into intelligent watermark. In order to satisfy the intelligent watermark concept, we mixed the given watermark with the selected features of the cover, in order to get the new watermark (intelligent watermark). This intelligent watermark is used to distort the watermarked cover if any attacking has been done on it, and the attacker couldn't benefit the watermarked cover. In this paper we took the vector map of GIS data as a case study for our scheme. In the future works, some media can be used in this approach, such as image, audio, video, text, etc.

REFERENCES

[1] Chaudhari, Bharati P., and A. K. Gulve, "Approaches of Digital Image Watermarking Using ICA", Proceedings of ISCET. Punjab, India, 2010.

[2] J.Kim, S. Won, W. Zeng, and S. g Park, "Copyright Protection of Vector Map Using Digital Watermarking in the Spatial Domain", 7th International Conference on Digital Content, Multimedia Technology and its Applications (IDCTA), Pages: 154 - 159, Aug. 2011.

[3] Lu-Ting, KoJwu-E Chen, Yaw-Shih, Shieh, Tze-Yun Sung, "A Novel Fractional Discrete Cosine Transform Based Reversible Watermarking for Biomedical Image Applications", International Symposium on Computer, Consumer and Control ((IS3C), Pages: 36 - 39, 2012.

[4] Mali MakarandLotan, .Suryavanshi Hitendra Eknath, Nitin N Patil, "Angle based digital watermarking of text document", World Journal of Science and Technology, pages: 171-175, 2012.

[5] Mireia Montanola Sales, Patrice RondaoAlface, Benoit Macq, "3D Objects Watermarking and Tracking of Their Visual Representations", The Third International Conferences on Advances in Multimedia, 2011.

[6] Nana Wang, Chaoguang Menb, "Reversible fragile watermarking for 2-D vector map authentication with localization", Computer – Aided Design Journal, Volume 44, Issue 4, Page: 320-330, April 2012.

[7] Qijun Guo,Yanbin Zhao, Pingpan Cheng, Fengming Wang, "An Audio Digital Watermarking Algorithm Against A/D And D/A Conversions Based on DCT domain", 2nd International Conference onConsumer Electronics, Communications and Networks (CECNet), Pages: 871 – 876, 2012.

[8] Smitha Rao M.S, Jyothsna A.N, Pinaka Pani. R, "Digital Watermarking: Applications, Techniques and Attacks", International Journal of Computer Applications (0975 – 8887), Volume 44– No.7, April 2012.

[9] Xiamu Niu, Chengyong Shao, Xiaotong Wang, "a survey of digital vector map watermarking", International Journal of Innovative Computing, Information and Control (ICIC), Volume 2, Number 6, pages: 1301-1316, December 2006.

[10] Yasser Dakroury, Ismail Abd El-ghafar, Ashraf Tammam, "Protecting GIS Data Using Cryptography and Digital watermarking", International Journal of Computer Science and Network Security (IJCSNS), VOL.10 No.1, January 2010.

Tawfiq A. Abbas received his BsC in computer science from the Basrah University in 1984, and also his MsC from the same university and in the same field in 1990. He received his Ph.D in computer science from university of technology in 2004. Prof. Dr. Abbas is the dean of Information Technology College at University of Babylon. His research interests include image processing, image compression, Steganography, and digital watermarking.

MajidJ.Jawad was born in 1967 at Babylon town, Iraq. He received his B.Sc in computer science from the University of Technology in 1991, and also his M.Sc. from the same university and same field in 2003. Now, he is a lecturer in the Babylon University and Ph. D student in the Babylon University-College of Science-Computer Science Dept. His research interests include image processing, Steganography, and digital watermarking in vector and raster maps.