



Proposed New Watermarking Approach for Vector Image

TAWFIQ A. ABBAS* and MAJID J.JAWAD¹

*Dean of Information Technology, College - Babylon University, (Iraq).

¹College of Science- Computer, Science dep.- Babylon University, (Iraq).

Corresponding author E-mail : {tawfiqasadi63 , majid_al_sirafi }@yahoo.com

(Received: May 29, 2013; Accepted: June 06, 2013)

ABSTRACT

While the transmission technology of data is increases rapidly, the technology to protect these from unauthorized users need to be enhanced. There are several technologies have used such as cryptography, but this technology don't provide efficient solution. Digital watermarking technology can provide efficient solution to the above crucial problem. Digital watermarking is applied in several media such as image, audio, video, text. 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 a new watermarking concept called intelligent watermarking. We took vector map of GIS (Geographic Information System), as case study. 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 combining these features with external watermark in order to get the intelligent watermark. Third embedding 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 decomposing the intelligent watermark into features and external watermark. Third reversing 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.

Key words :Intelligent Watermark; Copyright Protection;GIS; Digital Vector Map.

INTRODUCTION

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 proposed algorithm is presented .Experimental results and capability analyses are shown in Section 3. Conclusions and future works are drawn in Section 4.

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 is aim to remove the watermark or prevent the extraction of it. So, in this case, the owner can't 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 is consists of two stages.

Embedding the Watermark

This stage can be listed in the following steps:-

1. Extracting the features from the cover, which 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

$$iw = \text{comp}(ewm, f) \quad \dots(1)$$

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.

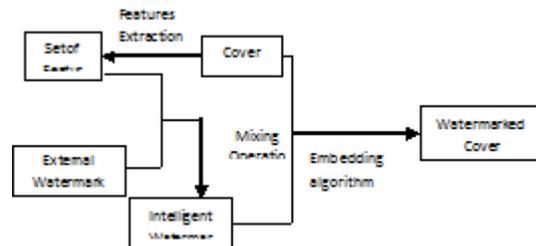


Fig. 1: Embedding watermark Operation

Extracting the Watermark and verification the result

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 $(ewm, f) = \text{decom}(eiwm) \quad \dots(2)$ where ewm, f, decom, eiwm is the external watermark, and the features , the decomposition function, the extracted intelligent watermark, respectively.
3. Reflecting the extracted features (which be selected after decomposition operation) on the features of watermarked media. So, if the features of watermarked cover is equal to the extracted features, this reflecting don'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 don't benefit the watermarked cover.

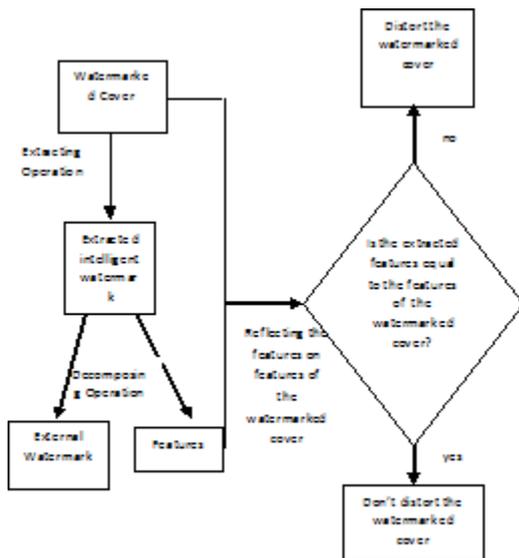


Figure 2: Extracting and verification operation



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



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

RESULTS

The background of the Vector Map

The data of GIS is 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 is normally composed of spatial data, attribution data, and some additional data

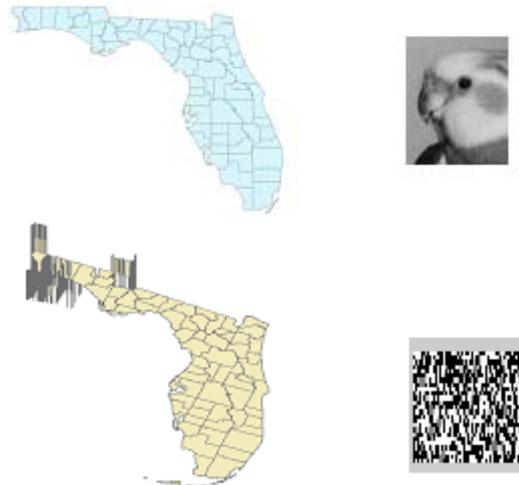


Fig. 5: (a) verified watermarked vector map without attacking (b) extracted watermark without attacking (c) verified watermarked vector map with attacking (rotation attack) (d) extracted watermark after attacking (rotation attack)

used as indices or extra descriptions, etc. Spatial data describes 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 is actually a sequence of coordinates of these vertices based on a certain geographical coordinate system. Attribution data describes 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 vertices⁹.

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.

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 this extracted features is composed with the external (original) watermark, by using formula 1

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.

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 don'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.

CONCLUSIONS

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 ISCEI. 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, SuryavanshiHitendraEknath, Nitin N Patil, "Angle based digital watermarking of text document", World Journal of Science and Technology, pages:171-175, (2012).
5. MireiaMontanola 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, ChaoguangMenb, "Reversible fragile watermarking for 2-D vector map authentication with localization", *Computer-Aided Design Journal*, **44 (4)**, Pages 320-330, (2012).
7. QijunGuo, Yanbin Zhao, PingpanCheng, Fengming Wang, "An Audio

- Digital Watermarking Algorithm Against A/D And D/A Conversions Based on DCT domain", 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Pages: 871 - 876, (2012).
8. Smitha Rao M.S, Jyothisna A.N, PinakaPani.R, "Digital Watermarking: Applications, Techniques and Attacks", *International Journal of Computer Applications* (0975 - 8887) ,**44(7)**, (2012).
9. XiamuNiu, 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.