IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. III (Nov.-Dec. 2016), PP 82-86
www.iosrjournals.org

Geo Spatial Data Hiding for Copy Right Protection Using 2x2 Block Approach

R. Anusha, M.V.S.N.Maheswar
(Cse, Pvpsit/ Jntuk, India)
(Cse, Pvpsit/ Jntuk, India)

Abstract: *As geospatial data is different from digital images, image watermarking evaluation methods cannot be directly applied to watermarked geospatial data. At present, watermarking algorithms are mainly focusing on robustness evaluation and error analysis. One of the important aspects related to vector data quality i.e. topological relationship inspection is neglected. An attempt has been made to incorporate invisible watermark in geospatial vector data using wavelet based watermarking algorithm and the resulted watermarked data has been evaluated in terms of polygon closure, topological relationship consistency and impact on visualization. Copyright protection on geospatial data results in security domain of various location data providers. To provide this a simple and enhancive 2x2 decomposed Hough man encoding fusion scheme is used. This results reconstruction of original polygon geospatial data and increment in performance metrics was observed.*
Keywords: *Geospatial data, Data quality, Watermarks.*

I. Introduction

Watermarking (data hiding) is the process of embedding data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or a detection algorithm. Watermarks can be embedded in the pixel domain or a transform domain. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. Invisibility refers to the degree of distortion introduced by the watermark and its effect on the viewers or listeners. Robustness is the resistance of an embedded watermark against intentional attacks, and normal A/V processes such as noise, filtering (blurring, sharpening, etc.), resampling, scaling, rotation, cropping, and lossy compression. Capacity is the amount of data that can be represented by an embedded watermark. The approaches used in watermarking still images include least-significant bit encoding, basic M-sequence, transform techniques, and image-adaptive techniques.

Typical uses of watermarks include copyright protection (identification of the origin of content, tracing illegally distributed copies) and disabling unauthorized access to content.Requirements and characteristics for the digital watermarks in these scenarios are different, in general. Identification of theorigin of content requires the embedding of a single watermarkinto the content at the source of distribution. To trace illegalcopies, a unique watermark is needed based on the location oridentity of the recipient in the multimedia network. In both ofthese applications, non-blind schemes are appropriate aswatermark extraction or detection needs to take place in a speciallaboratory environment only when there is a dispute regardingthe ownership of content. For access control, the watermark should be checked in every authorized consumer device used toreceive the content, thus requiring semi-blind or blind schemes.

Note that the cost of a watermarking system will depend on the intended use, and may vary considerably. Two widely used image compression standards are JPEG and JPEG2000. The former is based on the Discrete Cosine Transform (DCT), and the latter the Discrete Wavelet Transform (DWT). In recent years, many watermarking schemes have been developed using these popular transforms.In all frequency domain watermarking schemes, there is a conflict between robustness and transparency. If the watermark is embedded in perceptually most significant components, the scheme would be robust to attacks but the watermark may be difficult to hide. On the other hand, if the watermark is embedded in perceptually insignificant components, it would be easier to hide the watermark but the scheme may be least resistant to attacks. In image watermarking, two distinct approaches have been used to represent the watermark. In the first approach, the watermark is generally represented as a sequence of randomly generated real numbers having a normal distribution with zero mean and unity variance. This type of watermark allows the detector to statistically check the presence or absence of the embedded watermark. In the second approach, a picture representing a company logo or other copyright information is embedded in the cover image. The detector actually reconstructs the watermark, and computes its visual quality using an appropriate measure.Image watermarking algorithms can be classified into two categories spatial domain techniques(spatial watermarks) and frequency domain techniques(spectral watermarks). The spatial domain directly modifies the intensities are color values of

some selected pixels while the frequency domain modifies the values of some transformed coefficients(Discrete cosine transforms "DCT", discrete wavelet transforms "DWT").

II. Literature Review

2.1. Robust digital watermarking of color images: Recent researchers on secure digital watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and robustness of a watermarking scheme. In this approach, watermark is created from the content of the host image and discrete wavelet transform (DWT) is used for embedding watermarks, since it is an excellent time frequency analysis method which can be adapted well for extracting the information content of the image [9].To take the advantage of localization and multi-resolution property of the wavelet transform,[11] proposed wavelet tree based watermarking algorithm. In this approach, the host image is transformed into wavelet coefficients using a discrete-time wavelet transform (DTWT). The watermark is embedded in the wavelet coefficients which are grouped into super trees. Each watermark bit is embedded using two super trees.

Depending on the value of the watermark bit, one of the super trees is quantized with respect to a quantization index in such a way that the two super trees exhibit a large enough statistical difference, which can be extracted for obtaining decision. As each watermark bit is embedded in various frequency bands and the information of the watermark bit is spread throughout large spatial regions, therefore the watermarking technique is robust to attacks in both frequency and time domains. This technique is useful for removal of high-pass details in JPEG compression and robust to time domain attacks such as pixel shifting and rotation. In addition to copyright protection, the proposed watermarking scheme can also be applied to data hiding or image authentication.

2.2. Discrete-wavelet transform based multiple watermarking algorithms: In this approach, two important tools encryption and watermarking can be used to prevent unauthorized consumption and duplication. The watermark is embedded into LL and HH sub bands to improve the robustness. [12] This approach is useful in such a way that embedding the watermark in lower frequencies is robust to a group of attacks such as JPEG compression, blurring, adding Gaussian noise, rescaling, rotation, cropping, pixilation, sharpening and embedding the watermark in higher frequencies is robust to another set of attacks such as histogram equalization, intensity adjustment, gamma correction. To protect the copyright technique to enhance the security. This technique is useful for digital watermarking in DEM (digital elevation mode) data, which effectively protects the copyright of DEM data and avoids the unauthorized user. As wavelet coefficient set is embed watermark information, therefore the bit is inserted in the high activity texture regions with the maximum strength of Just Noticeable Distortion (JND) tolerance of Human Visual System (HVS) that makes the digital watermark robust. The watermark is permutated using Arnold transform and is embedded by modifying the coefficients of the HH and LL sub bands. In this approach, an integer wavelet based multiple logo-watermarking schemes for copyright protection of digital image is presented. A visual meaningful binary logo is used as watermark. The process of watermark embedding is carried out by transforming the host image in the integer wavelet domain. To construct a blind watermarking scheme, wavelet coefficients of HH and LL bands are modified depending on the watermark bits. To add the security, permutation is used to preprocess the watermark. [14] In addition, watermarking in DWT domain has drawn extensive attention for its good time-frequency features and its accurate matching of the human visual system (HVS).

2.3. Watermarking algorithms based on wavelet basis: One of them is based on optimization scheme using group-amplitude quantization and the other embeds information by energy-proportion scheme. [15] Therefore, normalized energy is used instead of probability which rewrites the entropy in information theory as energy proportion function. [16] In which the watermarks used are binary images. Although, in one of them a spread-spectrum technique is used to spread the power spectrum of the watermark data, in the two others, watermarking methods are based on a combination of spread spectrum and quantization. In which the code-division multiple access (CDMA) encoded binary watermark, adaptively is embedded into the third level detail sub-band of DWT domain. [17] It can be inferred from the literature survey that many of the algorithms proposed met the imperceptibility requirement quite easily but robustness to different image processing are mainly applied to content authentication attacks is the key challenge and the algorithms in literature addressed only a subset of attacks. In this approach, the watermark is embedded according to two keys [5]. The first key is used to embed a code bit in a block of pixels. The second bit is used to generate the whole sequence of code bits. The watermark is embedded in spatial domain by adding or subtracting a random digital pattern to the given image signal depends on the local energy distribution. The embedding depth level depends on the spectral density distribution of DCT coefficients and on the JPEG quantization table and inserts the watermark in the low frequency component. The depth label consists of a set of bits that are embedded locally in a rectangular set of blocks and it is repeated over the entire image. After detecting individual bits, the retrieve label is verified by performing a XOR operation to the watermark code.

III. Methodology

The main disadvantage of this technique is that while allowing lossy detection, even in the presence of corruption, it keeps the level of false positive detection to a minimum since the found signature has to go through detection step of positive identification to be called detected. The detector step aims at ensuring the maximum exactitude in the detection of the owner identification key and, as said previously, minimizing the number of false positive detection. The results presented later on should convince the reader of the performance of our decoder.

3.1 Algorithm

Step1: Original image is divided into multiples of2x2 blocks.
Step2: Each 2x2 block is converted into 3x3 blocks using interpolation.
Step3: Logarithmic values of these new elements are taken and stored in a variable. These values are used for the selection of length of watermark bits to be chosen.
Step4: Now the key should be added.

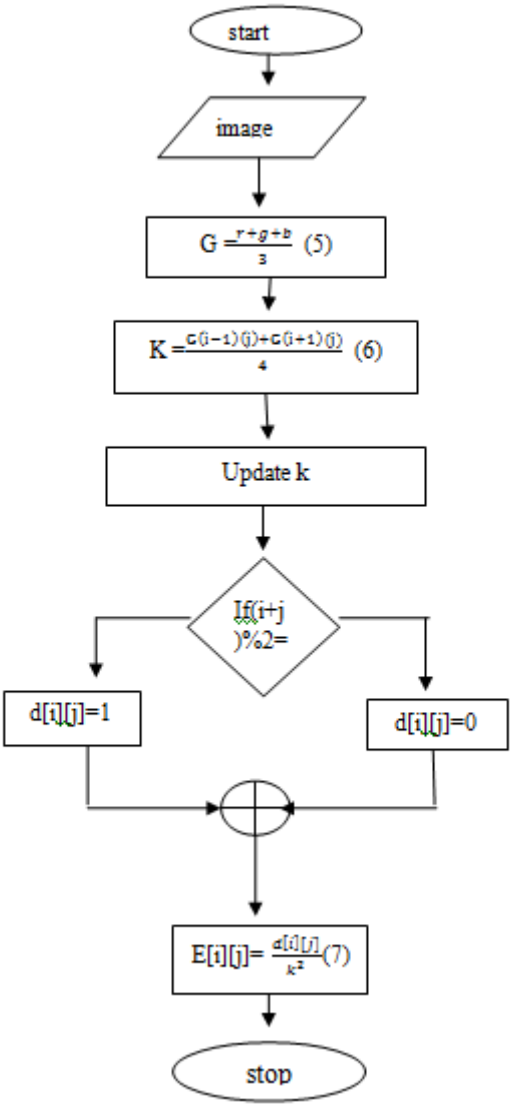

Figure 1: Proposing Flowchart

Step5: Bit stream of watermarkchosen according to log valuesand calculate equivalentdecimal values.
Step 6: The decimal values of those bit streams are added withthe new elements of 3x3 blocks.
Step7: This process is repeated for every 2*2 block until the watermark bits are embedded into the original image. Thus watermarked image is formed.

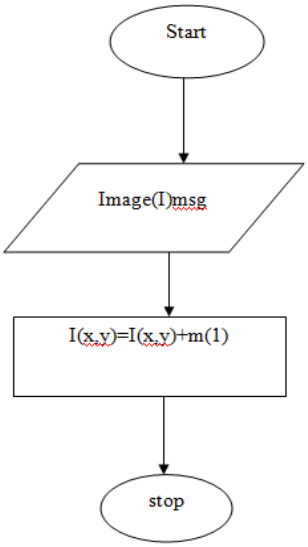

Figure3.2: Watermarking between image and data bits

A high capacity data hiding scheme is proposed for binary images authentication based on the interlaced morphological wavelet transforms. The relationship between the coefficients obtained from different transforms is utilized to identify the suitable locations for watermark embedding such that blind watermark extraction can be achieved. Two processing cases that are not intersected with each other are employed for orthogonal embedding in such way that are not only can the capacity be significantly increased, but the visual distortion can also be minimized. Results of comparative experiments with other methods reinforce the present scheme's superiority in being able to attain larger capacity while maintaining acceptable visual distortion and low computational cost. The goal of authentication is to ensure that a given set of data comes from a legitimate sender and the content integrity is preserved .Hard authentication rejects any modification made to a multimedia signal,whereas soft authentication differentiates legitimate processing from malicious tampering. This paper focuses on hard authenticator watermark-based authentication. Specifically, we investigate the problem of data hiding for binary images in morphological transform domain. Generally speaking, data hiding in real-valued transform domain does not work well for binary images due to the quantization errors introduced in the pre/post- processing. In addition; embedding data using real-valued coefficients requires more memory space. The idea of designing an interlaced transform to identify the embeddable locations is motivated by the fact that some transition information is lost during the computation of a single transform and there is a need to keep track of transitions between two and three pixels for binary images data hiding. Specifically, we process the images based on 2 X 2 pixel blocks and combine two different processing cases that the flip ability conditions of one are not affected by flipping the candidates of another for data embedding, namely "orthogonal embedding".

IV. Conclusion

Data hiding a vast area where data needs to hidden in various in digital image processing this came into existence by crypptography, steganography and watermarking. For geo-spatial data providers copy right theories are mandatory. This needs to be associated with change of security, here in this approach wavelet based 2X2 block encryption mode is developed and simulated. The major improvement is Time of Execution and non-complex data hiding scheme. And in future work we can replace this algorithm by using multiplication factor algorithms to reduce complexity.

References

[1]. *Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.*

[2]. *Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.*

[3]. *M. Shensa, "The discrete wavelet transform: Wedding the a trous and mallat algorithms," IEEE Transactions on Signal Processing,vol. 40, no. 10, pp. 2464–2482, 1992.*

[4]. *Mitchell D. Swanson, Mei Kobayashi, Ahmed H. Tewfik, "Multimedia Data Embedding and Watermarking Technologies", Proceedings of the IEEE, 86(6):10641087, June 1998*

[5]. *F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," Proc. Int. Conf. on Image Processing, Oct. 1998, vol. I, pp. 450-454.*

[6]. *Yuan Y., Huang D., Liu D., "An Integer Wavelet Based Multiple Logo- watermarking Scheme", In IEEE, Vol-2, pp. 175-179, 2006.*
[7]. *N. Ahmed, T. Natarajan, and K. Rao, "Discrete cosine transform," IEEE Transactions on Computers, vol. 100, no. 1, pp. 90–93, 1974.*
[8]. *P. Bas, J. Chassery, and F. Davoine, "Using the Fractal Code to Watermark Images," Proc. IEEE Int. Conf. on Image Processing, vol. I, Oct. 1998, pp. 469-473.*
[9]. *Reddy R., et al, "Robust Digital Watermarking of Color Images under Noise Attacks", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.*
[10]. *Wang Y., Doherty J.F., Dyck V.R.E., "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Transactions, Image Processing, 11 pp. 77-88, 2002.*
[11]. *Wang S.H., LinY.P., "Wavelet Tree quantization for copyright protection for watermarking", IEEE Transactions, Image Processing, pp. 154-165, 2002.*
[12]. *Tao P., Eskicioglu A.M., "A robust multiple watermarking scheme in the discrete wavelet transform domain", Proceedings of the SPIE, Vol. 5601, pp. 133-144, 2004.*
[13]. *Luo Y., et al. "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp. 1096-1103, 2005.*
[14]. *Lin Q., Lin Z., Feng G., "DWT based on watermarking algorithm and its implementing with DSP", IEEE Xplore, pp. 131-134, 2009.*
[15]. *Chen, S.T., Huang, H.N., Chen, C.J., Wu, G.D., 'Energy-proportion based scheme for audio watermarking', IET Signal Process., 2010, 4,(5), pp. 576–587.*
[16]. *Preda, R.O., Vizireanu, D.N., 'A robust digital watermarking scheme for video copyright protection in the wavelet domain', Measurement, 2010, 43, (10), pp. 720– 1726.*
[17]. *Deng, N., Jiang, C.S., 'CDMA watermarking algorithm based on wavelet basis'. Proc. 9th Int. Con. Fuzzy Systems and Knowledge Discovery, May 2012, pp. 2148– 2152.*
[18]. *Wu, X., Hu, J., Gu, Z. and Huang, J "A secure semi fragile watermarking for image authentication based on integer wavelet transform with parameters" Conferences in Research and Practice in Information Technology Series; Vol. 108, 2005.*
[19]. *Ho, C.K. and Li, C.T. Semifragile watermarking scheme for authentication of JPEG images. Proceeding of the IEEE international Conference on Information Technology: Coding and Computing, I, Pp. 7 – 11 2004.*