Volume 1, No. 3, October 2010
Journal of Global Research in Computer Science
RESEARCH PAPER
Available Online at www.jgrcs.info
ISSN-2229-371X

DATA HIDING IN BINARY IMAGES

Rupali D Kasar[1] and Bharti W. Gawali[2]

Dr. Babasaheb Ambedkar Marathwada University,Aurangabad India
rupalikasar1@gmail.com
bharti_rokade@yahoo.co.in

Abstract- In this paper, we will overview use of data hiding techniques in binary images. The interest in data hiding has raised with the recent activity in digital copyright protection schemes. The embedding capacity is the major concern in a data-hiding scheme. Several methods for hiding data in specific types of binary images have been proposed. Digital watermarking techniques are used to address digital rights management, protect information, and conceal secrets. This paper will review recent developments in data hiding techniques of binary images.

Keywords: Datahiding, digital watermarking, authentication, security, steganography, annotation, authentication, binary image.

INTRODUCTION

Data hiding in binary image, though difficult, is getting higher demands from our everyday life. It is secretly embedding data in graphics images and other file types. It is similar to compression, but distinct from encryption. Its goal is not to restrict or regulate access to the host signal, but rather to ensure that embedded data remain inviolate and recoverable. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove.

Data Hiding/Watermarking Techniques classification

Digital watermarking techniques can be classified in several ways. Figure 1. Shows data hiding techniques classification. Broadly watermarking can be divided into three areas. They are:
Fragile and robust watermarks
These can be two parts depending on different applications [1]. A digital watermark is called robust with respect to transformations if the embedded information can reliably be detected from the marked signal even if degraded by any number of transformations. Robust watermarks are useful for copyright and ownership assertion purposes. They cannot be easily removed and should resist common image-manipulation procedures such as rotation, scaling, cropping, rightness/contrast adjusting, lossy compression, printing, scanning, etc. On the other hand, fragile watermarks (or authentication watermarks) are easily corrupted by any image processing procedure. A watermark is called fragile if it fails to be detected after the slightest modification.

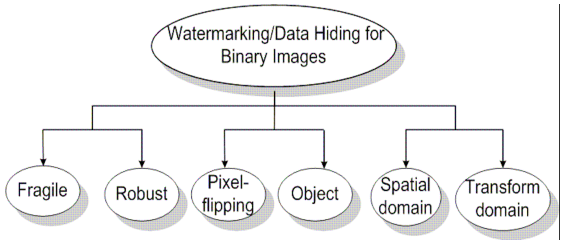

Fig 1: Data Hiding/watermarking Techniques for Binary Images classification

PIXEL-FLIPPING AND OBJECT-BASED TECHNIQUES

These techniques are depending on whether the watermark embedding is done in pixel level or object level. Specifically, a pixel-flipping technique encodes a message bit by flipping a pixel from white to black or vice versa, whereas an object-based technique encodes a message bit by modulating the spaces or features among characters and words.

SPATIAL AND TRANSFORM DOMAIN TECHNIQUE

In DSP, most commonly digital signals are studied in time or spatial domain (multidimensional signals) and frequency domains. These techniques are based on the domain where data hiding occurs. In spatial watermark is embedded by directly modifying the pixel values thus operate directly on pixels of input image. In transform domain watermark embedded in the transform space by modifying coefficients.

DIGITAL WATERMARKING

Digital watermarking is the process of embedding information into a digital signal. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy [2].

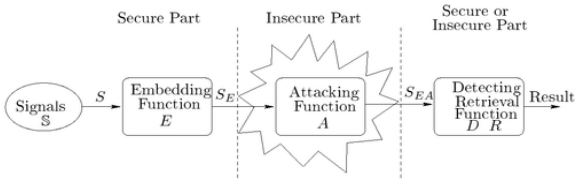

Fig. 2:Watermarking life-cycle phases

A watermarking life cycle is usually divided into three distinct phases.
i) Embedding, ii) Attack iii) Detection.

1) Embedding
In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person.

2) Attack

If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications.

3) Detection

Detection (often called extraction) is an algorithm, which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was Unmodified during transmission, then the watermark is still present and it can be extracted.

DATA HIDING TECHNIQUES

A significant number of data hiding techniques have been reported in recent years in order to create robust digital watermarks. Among all the existing techniques for digital colour and gray scale images, not all of them can be directly applied to binary text images. The problem is the fact that changing pixel values in a binary document could introduce irregularities that are very visually noticeable.

Q.Mei&E.K.Wong [3] proposed data hiding technique for binary text documents that embed data in the 8-connected boundary of a character. A fixed set of pairs of five-pixel long boundary patterns for embedding data is identified. The duality property of the *Add-Delete* patterns is used here. One of the patterns in a pair requires *deletion* of the centre foreground pixel, whereas the other requires the *addition* of a foreground pixel. A unique property of the proposed method is that the two patterns in each pair are dual of each other. Changing the pixel value of one pattern at the centre position would result in the other. This property allows easy detection of the embedded data without referring to the original document, and without using any special enforcing techniques for detecting embedded data. The duality property of Add-Delete patterns allows easy extraction of hidden data without using complicated enforcing technique. It is useful for annotating messages in text document and for detecting alterations.

A stegnography scheme for hiding a piece of critical information in a host binary image. This scheme ensures that, in each $m \times n$ image block of the host image, as many as $[\log_2(mn+1)]$ bits can be hidden in the block by changing at most two bits in the block. This improves the problem of CPT scheme. Although at most two bits can be modified in each host block, there is no control on the quality of the image after modification. In its capability to maintain higher quality of the host image after data hiding by sacrificing some data hiding space. The scheme can still offer a good data-hiding ratio. It ensures that, for any bit that is modified in the host image, the bit is adjacent to another bit, which has a value equal to the former's new value. Thus, the hiding effect is quite invisible [5].

A novel blind data hiding method for binary images authentication is mainly based on "connectivity-preserving" criterion. It aims at preserving the connectivity of pixels in a local neighbourhood. No side information is required for the watermark retrieval due to the invariant feature of the data embedding process. The "flippability" of a pixel is determined by imposing three transition criteria in a 3x3-moving window centered at the pixel. The "embeddability" of a block is invariant in the watermark embedding process; hence the watermark can be extracted without referring to the original image. The "uneven embeddability" of the host image is handled by embedding the watermark only in those "embeddable" blocks. The locations are chosen in such a way that the visual quality of the watermarked image is guaranteed. Different types of blocks are studied and their abilities to increase the capacity are compared. The problem of how to locate the "embeddable" pixels in a block for different block schemes is addressed which facilitates the incorporation of the cryptographic signature as the hard authenticator watermark to ensure integrity and authenticity of the image. Comparisons with prior methods show the superiority of the proposed scheme. A smaller block size is chosen in order to increase the data hiding capacity. The fixed 3x3 blocks, non-interlaced and interlaced block schemes are studied and the capacities achieved using different types of blocks are compared. Different types and sizes of block can be chosen for different applications. The problem of how to locate the "embeddable" pixels in a block for different block schemes is addressed, which facilitates the incorporation of the cryptographic signature as the hard authenticator watermark such that authenticity and integrity of the image are ensured. This scheme can be applied to a wide variety of binary images authentication. It achieves larger capacity compared with existing [3], [6], [7], [8] methods. The problem of how to locate the "embeddable" pixels and how to extract the watermark blindly are also addressed. Lower computational complexity (e.g. compared with [6], [10]) also defines visual quality preserving rules.

H. Lu, X. Shi introduced distance-reciprocal distortion measure (DRDM) method and visual quality preserving rule was defined. This distortion measure is for binary document images. This measure is derived from the observation that for binary document images, the distance between pixels plays a major role in their visual interference, and it is called the distance-reciprocal distortion measure. It is based on the reciprocal of distance that is straightforward to calculate. It is proved that the proposed distortion measure matches well to subjective evaluation by human visual perception. This measure is useful in a wide range of applications involving visual distortion in digital binary document images, such as watermarking, data hiding and lossy compression. However, this distortion measure is not suitable for halftone (dithered) images, in which black and white pixels are well interlaced and graininess is desired. In this case, the weight matrix elements should be proportional to the distance rather than its reciprocal [15].

Interest in multi resolution techniques for signal processing and analysis is increasing steadily. An important instance of such a technique is the so-called pyramid decomposition scheme. Multi- resolution signal decomposition schemes provide convenient and effective ways to process information. Pyramids, wavelets are among the most common tools for constructing multi resolution signal decomposition schemes.1-D morphological binary wavelet transform (*MBWT*); the morphological binary wavelet transform can be used to track the transitions in binary images by utilizing the detail coefficients. One rather intuitive idea in employing the morphological binary wavelet transform for data hiding is to use the detail coefficients as a location map to determine the data-hiding locations.

APPLICATION OF DIGITAL WATERMARKING

Digital watermarking and data hiding techniques have been proposed for a variety of digital media applications, including copyright protection, copy control, annotation, authentication, feature tagging and authentication. Recently authentication of digital document has made great interest due to wide applications in hand written signatures. Digital books, business document, personal document, maps and so on [3].

COPYRIGHT PROTECTION

This is the most prominent application of watermarking which embed information about the owner to prevent others from claiming copyright. Copy right protection systems are intended to prevent or deter unauthorized copying of digital media.A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property. This is the watermarking scenario where the message is the watermark. The "watermark" can be a relatively complicated structure. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified [4]. Detection of an embedded watermark is performed by a statistical, correlation, or similarity test, or by measuring other quantity characteristic to the watermark in a stego-image. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent surge of interest in digital stegnography and data embedding.

AUTHENTICATION

Authentication is an added security measure used to prove that someone is what they say they are before access is granted to confidential information. Watermarks may be used for certification, authentication, and conditional access. Certification is an important issue for official documents, such as identity cards or passports. Example on the identity number "123456789" is written in clear text on the card on left side and hidden as a digital watermark in the identity photo. Therefore switching or manipulating the identity photo will be detected.Authentication watermarking can be further classified into hard authentication and soft authentication. Hard authentication is the validation of content that does not allow any modifications. That means a single bit change in the test image will trigger an alarm that indicates the content is unauthentic. "Hard" image authentication is highly sensitive and dependent on the exact value of image pixels, whereas "Soft" image authentication is sensitive just to content modification and serious image quality tampering. Authentication is the service of ensuring whether a given block of data has integrity (i.e. the associated content has not been modified) and is from the legitimate sender.

FEATURE TAGGING

Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the image also copies the entire embedded features .the cover signal is required during the detection process.

In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark. In invisible watermarking information is added as digital data to audio, picture or video. It cannot be perceived as such.

CONCLUSION

An overview of data hiding for binary images have presented along with applications that can benefit from the technology. Basic features of watermarking system are also discussed, followed by various approaches in data embedding and hiding. Most data-hiding techniques for binary images are based on spatial domains, choosing data-hiding locations by employing pairs of contour edge patterns means by changing pixel values along the non-smooth portions of character boundaries, edge pixels visual distortion tables and defining visual Quality-preserving rules. However, the capacities of the existing algorithms are not large enough, especially for small images. The existing large capacity algorithm does not have good visual quality of the watermarked image and the computational load is relatively high. Data hiding in real-valued transform domain does not work well for binary mages due to the quantization errors introduced in the pre/post-processing. Whereas embedding data using real-valued coefficients requires more memory space. Morphological binary wavelet transform can be used to track the transitions in binary images by utilizing the detail coefficients as a location map to determine the data-hiding locations.

REFERENCES

[1] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia data embedding and watermarking technologies," Proceedings *of the IEEE*, Vol. 86, No. 6, pp. 1064-1087, June 1998.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom*, Digital Watermarking*. San Mateo, CA: Morgan Kaufmann, 2001.

[3] Q. Mei, E. K. Wong, and N. Memon, "Data hiding in binary text document," in *Proc. SPIE*, 2001, vol. 4314, pp. 369–375.

[4] H. Lu, X. Shi, Y. Q. Shi, A. C. Kot, and L. Chen, "Watermark embedding in DC components of DCT For binary images," in *Proc., IEEE Workshop on Multimedia Signal Processing*, Dec. 9–11, 2002, pp. 300–303.

[5] Yu-Yuan Chen, Hsiang-Kuang Pan, and Yu-Chee Tseng," A Secure Data Hiding Scheme for Two- Color Images" Email: yctseng@csie.ncu.edu.tw .

[6] Y. C. Tseng and H.-K. Pan, "Data hiding in 2-color images",*IEEE Trans. Comput.*, vol. 51, no. 7, pp. 873–878, Jul. 2002.

[7] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," *IEEE Trans. Multimedia*, vol. 6, no. 4, pp. 528–538, Aug. 2004.

[8] H. Y. Kim and R. L. de Queiroz, "Alteration-locating authentication watermarking for binary images," in *Proc. Int. Workshop Digital Watermarking*, 2004, pp. 125–136.

[9] K.-F. Hwang and C.-C. Chang, "A run-length mechanism for hiding data into binary images," in Proc. Pacific Rim Workshop on Digital Steganography, Kitakyushu, Japan, Jul. 2002, pp. 71–74.

[10] H. Yang and A. C. Kot, "Pattern-based date hiding for binary images authentication by connectivity-preserving," IEEE Trans.Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007.

[11] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," Proc. IEEE, vol. 87, no. 7, pp. 1167–1179, Jul. 1999.

[12] H. J. A. M. Heijmans and J. Goutsias, "Nonlinear multiresolution signal decomposition schemes -part II: Morphological wavelets," IEEE Trans. Image Process., vol. 9, no. 11, pp. 1897–1913, Nov. 2000.

[13] C.-Y. Lin and S.-F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," IEEE Trans. Circuits Syste. Video Technol., vol. 11, no. 2, pp. 153– 168, Feb. 2001.

[14] P. W. Wong and N. Memon, "Secret and public key image water marking schemes for image authentication and ownership verification," IEEE Trans. Image Process., vol. 10, no. 10, pp. 1593–1601, Oct. 2001.

[15] H. Lu, A. C. Kot, and Y. Q. Shi, "Distance-reciprocal distortion measure for binary document images," IEEE Signal Process . Lett., vol. 11, no. 2, pp. 228–231, Feb. 2004.

