Research Article

BINARY TEXTUAL/DOCUMENTS IMAGE AUTHENTICATION BY EMBEDDING SECURITY CODE USING WAVELET TRANSFORM ENCODING

***Jatinderpal Singh and Mamta Garg**
Department of CSE, Adesh Institute, BMSC of Engineering (Muktsar) Punjab INDIA
**Author for Correspondence*

ABSTRACT

In the existing scenario, the digital images are scanned for their originality or tamper proofing by using the water marking algorithms. However, the water marking algorithms are normally suitable for high color resolution images and do not suit to the textual images i.e. binary images or black and white images. It is very tedious task to embed secret codes or authenticated code in the text images. Further, the task becomes more difficult for the smaller images. Therefore, ensuring the legality of the digital text documents becomes a big challenge in the existing digital communication world. Further, the text image i.e. document material should not be altered to the first recipient in the communication path so that the general/visible textual matter is reached to the person directly receiving the text image. However, the embedded or hidden data has to be retrieved from the text image for authenticating it's genuinely. In the proposed work, the digital text images are targeted for ensuring the authenticity using the high data embedding algorithm.

Key Words: *Water Marking, DWT, Embedded Data*

INTRODUCTION

The text image i.e. document material should not be altered to the first recipient in the communication path so that the general/visible textual matter is reached to the person directly receiving the text image. However, the embedded or hidden data has to be retrieved from the text image for authenticating it's genuinely. In the proposed work, the digital text images are targeted for ensuring the authenticity using the high data embedding algorithm.

Data hiding techniques have been proposed in a wide variety of applications, such as owner identification, content authentication, annotation, copy control, and covert communications. The required properties of a data-hiding system strongly depend on the applications. Recently, an increasingly large number of important documents such as legal documents, certificates and handwritten signatures have been digitized and stored in binary image form. This goes hand in hand with the aim of the paperless workspace, but it does come at the expense of security breaches especially if the document is transmitted over the internet.

It is becoming easier and easier to edit an image with the powerful image editing tools that is difficult to detect. To assist in maintaining and verifying the integrity of the digital documents as well as tampering detection are becoming a very important issue. Most prior works on image data hiding focus on color and grayscale images in which the pixels take on a wide range of values, slightly changing the color of a small amount of pixels causes no perceivable change for human eyes. But for binary images, hiding data is more difficult. Black and white are the only two colors in a binary image and arbitrarily flipping pixels in the non-edge regions of binary images will create dramatic difference.

Related Works

Generally speaking, hiding data in binary images can be done in three basic ways. The first class of approaches changes low-level features of image such as flipping pixels from black to white or vice versa to enforce specific configuration in a block (Wu and Liu, 2004; Tseng *et al.*, 2002).

The second class of approaches is usually for specific type of binary images, e.g. binary document images, which changes higher level features such as modifying the thickness of strokes, curvature, spacing, and relative positions (Maxemchuk and Law, 1997).

The third class of approaches is directly encoding the hidden information in flippable pixels which are shared by the sender and the receiver (Yang *et al.,* 2008). To achieve blind watermark extraction, this class of approaches should ensure that "embeddability" of the pixel is invariant in the embedding process. The drawback of the most existing schemes is that the capacities are not large enough, especially for the small size of images. Various types of binary images can be used as host images, including document images, halftone images, scanned figures, text and signatures. The goal of image authentication is to verify that an image has not been altered since it left a trusted party. If even a single bit has been changed, the image is regarded as inauthentic by exact authentication. The major advantages of the proposed scheme lies its larger capacity and better visual quality, which guarantee the authentication mark can be embedded in rather small images. Moreover, our proposed scheme with high capacity also can better serve for purpose of covert communications. Such data hiding techniques are called steganography. Comparisons of the visual quality of the proposed method with other methods proposed by Tseng *et al.,* (2002) and Yang *et al.,* (2008) are made. English text (EnglishText), Chinese text (ChineseText) and handwritten (HandWritten) are used in the experiments. The capacity achieved by Tseng's method for EnglishText, ChineseText and HandWritten are 1764, 1764 and 255 bits, respectively, as well as 3140, 3240 and 344 bits in Yang's method. The block size for Tseng's method is chosen such that larger capacity is obtained under the constraints that the watermarked image is of acceptable visual quality. To compare the visual quality, the proposed method embeds equal amount of data with Tseng's and Yang's methods. DRDM (Lu *et al.,* 2004) is an objective distortion measure for binary document images, which is used to evaluate the visual distortion of the watermarked images. From the study of literature, it has been observed that digital water marking is a good solution for landscape or high colorful images. As the embedding of secure or authentic data does alter the image visually. And also does not appear to the viewer. However, in case of textual image, digital water marking does not suit well as the embedding of water mark may appear visually and the security purpose is lost. Therefore, an invisible data hiding is required in case of digital stored documents (text documents) so that the original contents of digital text document are preserved without any tampering. In the proposed work, an algorithm is suggested for embedding data in spatial domain and frequency domain to digital documents. In spatial domain, data is embedded using the spatial coordinates of the image. While in frequency domain, dct coefficients of the image are used for embedding the data.

Image Decomposition using DWT

The input image is in JOEG format i.e. an rgb image. The image is converted to gray scale image using rgb2gray function in matlab. The gray image is now decomposed into LL, LH, HL and HH frequency sub-bands using the discrete wavelet decomposition at level-1 using the haar wavelet. The gray image is divided into 2x2 pixel block and the haar wavelet is implemented by using the following matrix computation:

$$\begin{pmatrix} f(i_1,j_1) & f(i_1,j_1) & f(i_1,j_1) & \cdots & f(i_1,j_n) \\ f(i_2,j_1) & f(i_2,j_1) & f(i_2,j_1) & \cdots & f(i_2,j_n) \\ \ldots\ldots & & & & \\ f(i_n,j_1) & f(i_n,j_1) & f(i_n,j_1) & \cdots & f(i_n,j_n) \end{pmatrix}_{NxN}$$

(Input Image)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2x2 Haar Wavelet Block

The LL, LH, HL and HH components are given by:

LL = (a + b + c + d)/√2 HL = (a-b) + (c-d)/ √2

LH = (a + b)-(c + d)/ √2 HH = (a-b)-(c-d)/ √2

The decomposed image may be viewed from the following structure in different sub bands.

LL$_1$ LL$_2$ LL$_3$ …. LL$_N$	HL$_1$ HL$_2$ HL$_3$ …. HL$_N$
LL$_1$ LL$_2$ LL$_3$ …. LL$_N$	HL$_1$ HL$_2$ HL$_3$ …. HL$_N$
LL$_1$ LL$_2$ LL$_3$ …. LL$_N$	HL$_1$ HL$_2$ HL$_3$ …. HL$_N$
..	..
..	..
LL$_1$ LL$_2$ LL$_3$ …. LL$_N$	HL$_1$ HL$_2$ HL$_3$ …. HL$_N$
LH$_1$ LH$_2$ LH$_3$ …. LH$_N$	HH$_1$ HH$_2$ HH$_3$ …. HH$_N$
LH$_1$ LH$_2$ LH$_3$ …. LH$_N$	HH$_1$ HH$_2$ HH$_3$ …. HH$_N$
LH$_1$ LH$_2$ LH$_3$ …. LH$_N$	HH$_1$ HH$_2$ HH$_3$ …. HH$_N$
..	..
..	..
LH$_1$ LH$_2$ LH$_3$ …. LH$_N$	HH$_1$ HH$_2$ HH$_3$ …. HH$_N$

Data Hiding in Host Image

The data to be hidden is inserted in the LL sub band image by using the following rule:

Ca(i, j)=ca(i, j)+k*W(i, j);

Where Ca is the embedded image. Ca(I, j) is the host image and w(i, j) is the data image. After embedding the data image, the embedded image is obtained by taking the inverse wavelet transform of Ca(i, j).

PSNR, ENTROPY AND MSE

PSNR: The peak-signal to noise ratio (PSNR) was used to evaluate the reconstructed image quality. The PSNR is defined as follows:

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{N\times N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left(f(i,j)-\hat{f}(i,j)\right)^2}dB,$$

where N × N is the size of the original image and f(i, j) and f(i, j) are the gray-level pixel values of the original and reconstructed images, respectively.

Entropy E: The expression of the information entropy of an image is given by:

$$H = -\sum_{i=0}^{L-1} p_i \ln p_i,$$

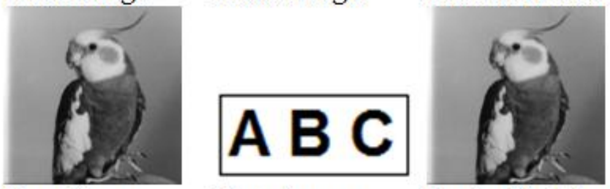
Where L denotes the number of gray level, pi equals the ratio between the number of pixels whose gray value equals i (0 to L - 1) and the total pixel number contained in an image. The information entropy measures the richness of information in an image. If pi is the const for an arbitrary gray level, it can be proved that the entropy will reach its maximum.

MSE: MSE is computed by the following formula:
MSE = ∑(I1(i, j) – I2(i, j)2 / N
Where I1 and I2 is the original and water mark images.

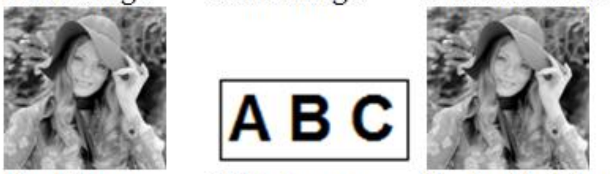
RESULTS AND DISCUSSION

Results

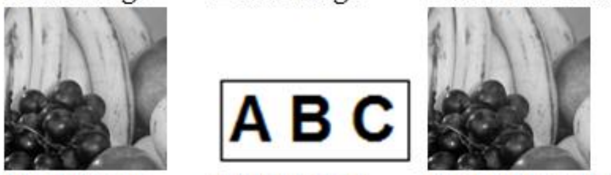
Host Image Data Image Embedded Image → Figure 1



Host Image Data Image Embedded Image → Figure 2



Host Image Data Image Embedded Image → Figure 3



Host Image Data Image Embedded Image → Figure 4

	Entropy		MSE	PSNR
Images	**Before WM**	**After WM**		
Figure 1	0.013	0.019	9.13	38.57
Figure 2	0.015	0.024	9.45	38.41
Figure 3	0.040	0.059	8.90	38.67
Figure 4	0.023	0.050	7.79	39.25

The proposed algorithm has been implemented on different host and data images. Above table shows the results obtained.

Conclusion

The data image embedded using the proposed technique shows a fair degree of hiding of the water mark in the image with 100% retrieval of the embedded data. Further, the result table shows that the embedded image has good robustness towards the water mark insertion as the entropy and MSE both are towards their lower side. The PSNR value shows the noise removal at a better scale as the image is de-noised using the wavelet decomposition during the secure data insertion.

REFERENCES

Bierbrauer J and Fridrich J (2008). Constructing good covering codes for applications in steganography, *LNCS Transactions on Data Hiding and Multimedia Security*, Springer-Verlag **4920** 1-22.

Cohen G, Honkala I, Litsyn S and Lobstein A (1997). Covering Codes, Elsevier.

Fu MS and Au OC (2001). Halftone image data hiding with intensity selection and connection selection, *Signal Processing: Image Communication* **16** 909-930.

Lu H, Kot AC and Shi YQ (2004). Distance-Reciprocal Distortion Measure for Binary Document Images, *IEEE Signal Processing Letters* **11**(2) 228-231.

Maxemchuk NF and Low S (1997). Marking text documents. *Proceedings of ICIP'97*.

Tseng YC, Chen YY and Pan HK (2002). A secure data hiding scheme for binary images, *IEEE Transactions on Communications* **50**(8) 1227-1231.

Wu M and Liu B (2004). Data hiding in binary image for authentication and annotation, *IEEE Transactions on Multimedia* **6**(4) 528-538.

Yang H, Kot AC and Rahardja S (2008). Orthogonal data embedding for binary images in morphological transform domain-a high-capacity approach, *IEEE Transactions on Multimedia* **10**(3) 339-351.