

Watermarking of Grayscale Text Document Images using Histogram Swapping

Jayanth Silesh S, Anvitha Jaishankar and Rashmi N,
Prof.Saritha Chakrasali(Associate Proffessor),
Dept. of Information Science And Engineering,
BNM Institute of Technology, Bangalore, India.

e-mail: jayanthbiles@s@gmail.com, anvithaj90@gmail.com, rashmi04nagendra@gmail.com

Abstract— Digital watermarking is widely believed to be a valid means to discourage illicit distribution of information content. The various methods for text documents are limited because of the binary nature of text documents. In this paper, a novel watermarking scheme which induces an Invisible watermark on grayscale digital text document images is presented. A histogram based algorithm is developed. The watermarked images are resistant to various geometrical attacks like rotation, flipping, translation, aspect ratio changes and resizing and others.

Keywords- *Intensity Modification, Robust watermarking, Histogram modification, Geometrical attacks, Watermarking.*

I. INTRODUCTION

The last decade has witnessed the domination of digital media. The new digital reality provides users with many accommodations like high quality, manipulation of the context, creation of perfect duplicates, streaming over the internet etc. The electronic distribution of information is faster, less expensive, and requires less effort than making paper copies and transporting them. Nevertheless these technologies in combination with the World Wide Web enable the perfect copying and distribution of copyrighted material anywhere in the world with practically no cost. In addition, electronic copies are more akin to the original than paper copies. When an electronic copy is made, the original owner and the recipient have identical entities. A person with a photocopy of a journal and a person with the original bound journal may have the same information, but it looks and feels different. Illicit copies of electronic documents are likely to result in major loss of revenues. Therefore a significant problem of non authorized copying and distribution of digital text documents is raised. Also in certain cases the problem of authenticity and reliability is raised (like in medical or military implementations). Digital Watermarking is called to cope with some of these issues. Without methods which prevent or discourage illicit redistribution and reproduction of information content, copyright can be easily infringed. The primary goal of information protection is to permit proprietors of digital information (i.e., the artists, writers, distributors, packagers, market researchers, etc.) to have the same type and degree of control present in the "paper world."

There are primarily three types of text watermarking methods which have been developed previously. They are

- Line-Shift Coding – vertically shifts the locations of text lines to encode the document.
- Word-Shift Coding – horizontally shifts the locations of words within text lines to encode the document.
- Feature Coding – chooses certain text features and alters those features.

These three methods require the original unmarked text for decoding. The proposed method uses the histograms for watermarking and does not require the original text image for recovering the watermark.

II. PROPOSED WATERMARKING TECHNIQUE

The watermarking scheme has a good watermarked image quality that is almost invisible. It is applicable to all grayscale text document images and all image sizes. It is robust against geometrical attacks like rotation, flipping, aspect ratio changes and resizing, warping, shifting and has a good resistance to image tampering. The basic principle involved in this type of watermarking is the swapping of image intensities. The intensities in the histogram bins are selected based on a secret key or certificate. For embedding the signal, the intensities of the images are swapped. Images can be reverted back to its original, if the certificate is known.

A. Watermark embedding

Steps for embedding the watermark:

Step 1: Classify the intensities of the image into histogram bins. The intensities of the images range between 0-255 for grayscale images. Take the intensities in steps of 6. Thus, intensities ranging from 0-6 lie in histogram bin 1 and intensities ranging from 7-12 lie in histogram bin 2. Thus, we get a complete of 43 histogram bins. "Figure 1", shows the histogram for grayscale text document image.

Step 2: Choose the signal to be inserted. It must a sequence of zeros and ones. The secret key or the certificate is randomly generated. It must be in the range of 1 to 43. The size of the certificate must be same as the size of the signal inserted.

Step 3: Let variable 'a' hold the first element in the certificate. The 'a'th and the 'a+1'st bin in the histogram are compared(Figure 1). If both the histograms have the same value or zero, increment 'a' by 1.

Insert the signal 1 or 0 based on the following rules.

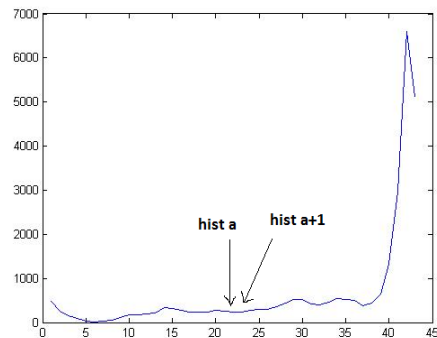


Figure 1. Histogram of original document

Rule 1 for embedding signal 0:

The condition $\mathbf{Hist(a)} < \mathbf{Hist(a+1)}$ must be satisfied. If not, go to step 4 to swap the histogram values of a^{th} & $a+1^{st}$ bins.

Rule 2 for embedding signal 1:

The condition $\mathbf{Hist(a)} > \mathbf{Hist(a+1)}$ must be satisfied. If not, go to step 4 to swap the histogram values of a^{th} & $a+1^{st}$ bins.

Step 4a:

Calculate the range of intensities by using the formula:
 $\text{“intensity1}=(a-1)*6\text{”}$ & $\text{“intensity2}=((a+1)-1)*6\text{”}$

All intensities that come under bin ‘a’, are: intensity1, intensity1+1, intensity1+2, intensity1+3, intensity1+4, intensity1+5.

Similarly, for bin ‘a+1’ are: intensity2, intensity2+1, intensity2+2, intensity2+3, intensity2+4, intensity2+5.

Step 4b:

The complete image is scanned and all the corresponding intensities are swapped, i.e. intensity1 will be swapped with intensity2 (intensity1 \leftrightarrow intensity2). Similarly, intensity1+1 will be swapped with intensity2+1 (intensity1+1 \leftrightarrow intensity2+1). This has to be done for all intensities: intensity+1, intensity+2, intensity+3, intensity+4, intensity+5.

Step 3 has to be repeated until all the elements in the certificate are exhausted. “Figure 2. & Figure 3.” show the original and watermarked image respectively. “Figure 3. & Figure 4.” show the watermark of the original and watermarked image respectively. “Figure 6.” shows the embedding flowchart.

B. Signal extraction

The secret key or the certificate is required to extract the signal from the watermarked image. As this is a blind watermarking technique, there is no need for the original image for recovering the signals inserted from the image but the secret key is required.

The steps for the extracting algorithm are as follows:

Step 1: The image is taken and the histogram is computed.

1. Introduction.

The objective here is to develop and i
 tions known as distributed microstructu
 fractured porous media. A fractured m
 permeable cells separated by a highly c
 microstructure models over more classic
 additional information associated with t
 such a medium the fractures account fi
 most of the storage occurs in the porous

Figure 2. Original image

1. Introduction.

The objective here is to develop and i
 tions known as distributed microstructu
 fractured porous media. A fractured m
 permeable cells separated by a highly c
 microstructure models over more classic
 additional information associated with t
 such a medium the fractures account fi
 most of the storage occurs in the porous

Figure 3. Watermarked image

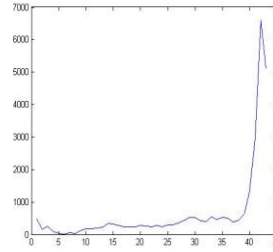


Figure 3. Histogram-Original

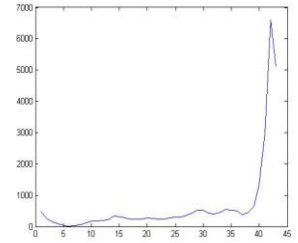


Figure 4. Histogram-Watermarked

Step 2: The first element in the secret key is taken as ‘a’ and the corresponding values of the histogram hist(a) and hist(a+1) are compared. If they are equal, then the values of ‘a’ & ‘a+1’ must be incremented by 1.

Each couple (a, a+1) correspond to a key. The following rules are applied.

If,

$\text{hist(a)} < \text{hist(a+1)}$; then the signal is 0.

$\text{hist(a)} > \text{hist(a+1)}$; then the signal is 1.

Step 2 has to be repeated until all the elements in the certificate are exhausted. The recovered signals are compared with the inserted signals to check the originality of the document.

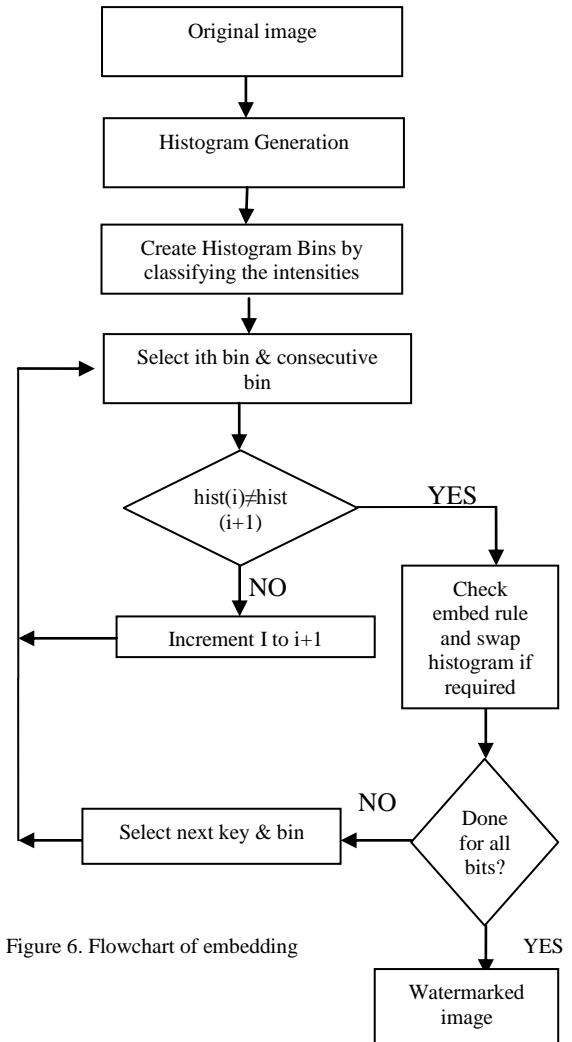


Figure 6. Flowchart of embedding

III. EXAMPLE

Consider 8 bits (1 0 1 0 1 0 1 0) to be embedded into a grayscale text document image. One histogram bin will have a range of 6 intensities. This is done to get a better quality histogram for swapping of intensities. Since 8 bits are embedded into the image secret key chosen should contain 8 elements. Consider the secret keys as: 21, 15, 6 and 40. This can be generated randomly.

Embedding signals: Since the first element in the signal is 1, follow rule 2 to embed and first key is 21, $hist(21)=600$ and $hist(22)=650$, $hist(21)$ and $hist(22)$ are swapped. If both the histograms have the same values or zero, then increment 'a' by 1. If they have histogram bin values $hist(a)=654$ & $hist(a+1)=654$, then, 'a' must be incremented by 1. Therefore, $a=22$ & $a+1=23$. This must be done until both 'a' and 'a+1' have different values. Repeat this process until all the elements in the secret key are exhausted. The swapping is done according to step 4 in the embedding process.

Intensity1=120, intensity2=126. Intensity1+1 is swapped with intensity2+1. Intensity1+2 is swapped with intensity 2+2 and so till all the intensities until intensity1+5 is swapped with intensity2+5.

Signal recovery: First element of the secret key(21) is considered and the histogram of the text document image is created according to step1 of the embedding process. If,

$hist(21) < hist(22)$; then the signal is 0.

$hist(21) > hist(22)$; then the signal is 1.

IV. EXPERIMENTAL RESULTS

The above algorithm can be applied to grayscale text document images. The algorithm will work in perfection if the histogram bins do not have too many zero values.

Experiments were conducted for more than 15 text images of different languages. "Table 1", shows the experimental results for the attacked watermarked images. Different attacks like noise, tampering and rotation of images were considered for the encoding of signals 1 0 1 0 1 0 1 0 and 0 1 0 1 0 1 0 1. "Figure7 to Figure 10" show the noised images.

"Graph 1." shows the accuracy level with the increase in the noise level. The x-axis shows the noise level in the image and the y-axis shows the accuracy percentage. The accuracy level goes on decreasing with the increase in the noise level. At a certain point the accuracy level becomes zero. This point is the threshold point. In our experiment the threshold point was found to be 0.8.

"Graph 2." shows the PSNR values for different noise levels. The PSNR values go on decreasing as the noise levels increase.

The PSNR values are the values when the watermarked image are attacked.



Figure 7. Watermarked image

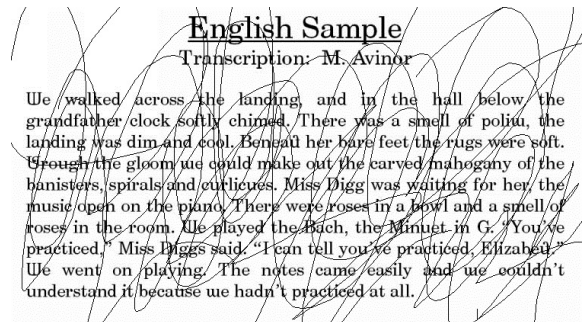


Figure 8. Tampered image



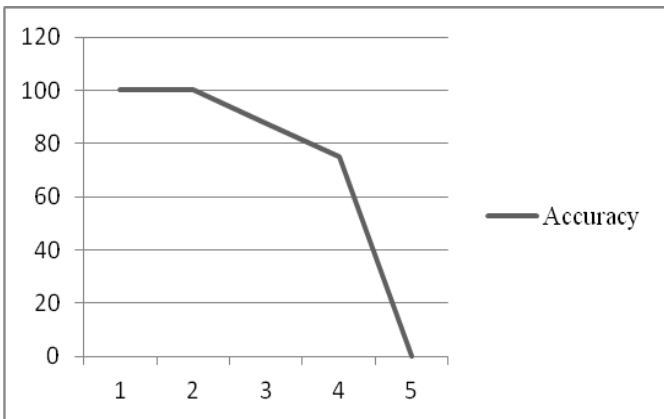
Figure 9. "Salt and pepper" noised image (0.08)



Figure 10. 180 degree rotated image

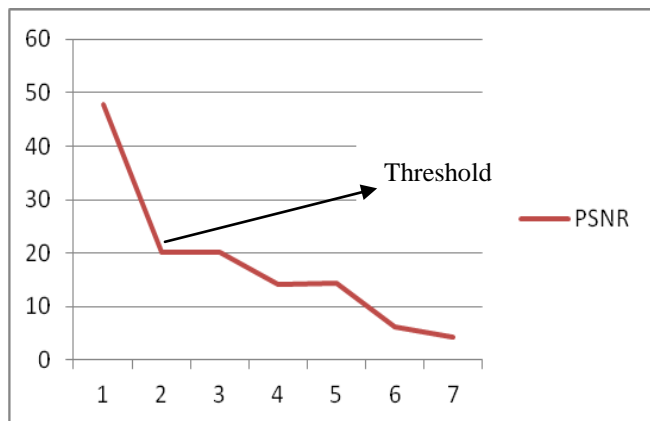
TABLE 1. TABLE SHOWING THE PSNR AND THE ACCURACY LEVELS OF THE WATERMARKED IMAGES.

Attack	Degree of Attack	Encoded Signal	Decoded Signal	PSNR	Accuracy
Watermarked Image	-	1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0	47.6641	100%
Noise(Salt & Pepper)	0.02	1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0	20.1881	100%
Noise(Salt & Pepper)	0.02	0 1 0 1 0 1 0 1	0 1 0 1 0 1 0 1	20.2460	100%
Noise(Salt & Pepper)	0.08	1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0	14.2154	100%
Noise(Salt & Pepper)	0.08	0 1 0 1 0 1 0 1	0 1 0 1 0 1 0 1	14.2944	100%
Noise(Salt & Pepper)	0.5	1 0 1 0 1 0 1 0	1 0 1 0 1 1 1 0	6.2872	87.5%
Noise(Salt & Pepper)	0.8	1 0 1 0 1 0 1 0	1 0 1 0 0 1 1 0	4.2480	75%
Tampering	1 st Degree	1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0	21.4516	100%
Tampering	2 nd Degree	1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0	14.0178	100%
Tampering	3 rd Degree	1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0	8.9003	100%
Rotating	180 Degree towards right	1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0	9.7319	100%



Graph 1. Showing the accuracy levels. X-axis: noise level. Y-axis: accuracy.

Graph 2. PSNR values, when attacked on Watermarked Image.



X-axis : noise level. Y-axis: PSNR value.

I. CONCLUSION

The encoded signal can be retrieved without the original document (blind watermarking). This scheme is highly resistive to any attack. Attacks such as "Salt & Pepper" can be resisted till a magnitude of 0.8 with decoding of about 75-100% accuracy.

II. COPYRIGHT FORMS AND REPRINT ORDERS

The Images used in the above paper are taken from www.google.com.

III. ACKNOWLEDGMENT

We are extremely thankful to **Dr.Sahana D Gowda & Asst.Prof Deepthi K Prasad** from BNM Institute of Technology, for their kind consent to be our guide and for providing their support, suggestions and unconditional guidance and their valuable time that helped us immensely in writing this paper. We are thankful for BNMIT for providing all the facilities which helped up publish this paper.

IV. REFERENCES

- [1]Chrysochos E., Fotopoulos V., Skodras A., Xenos M., "Reversible Image Watermarking Based on Histogram Modification", 11th Panhellenic Conference on Informatics with international participation
- [2](PCI 2007), Vol. B, pp. 93-104, 18-20 May 2007, Patras, Greece.
- [3]Fotopoulos V., Skodras A.: Digital image watermarking: An overview, invited paper, EURASIP Newsletter, ISSN 1687-1421, Vol. 14, No. 4, Dec. 2003, pp. 10-19 (2003).
- [4]Young-Won Kim and Il-Seok Oh, "Watermarking text document images using edge direction histograms", Science Direct , Pattern Recognition Letters 25 (2004) 1243–1251.
- [5]Joachim J. Eggers and Bernd Girod, "Quantization Watermarking", Proceedings of SPIE Vol. 3971
- [6] X.-G. Xia, C. G. Bonchelet, and G. R. Arce, "A multiresolution watermark for digital images," in Proceedings of the IEEE International Conference on Image Processing 1997 (ICIP 97), vol. 1, pp. 548–551, (Santa Barbara, CA, USA), October 1997.