IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

A Case Study on Water Marking with Implementation of Least Significant Bit coding (LSB)

N.S. Murti Sarma[1] and Santhosh[2]

Sreenidhi Institute of Science and Technology, Yamnampet, Medchal, Telangana[1]

Geetanjali College of Engineering and Technology, Keesara, Hyderabad[2]

Abstract: Watermarking technique is considered to compare the statistical performances of the retrieved images after inserting visible and invisible water marking. The results found are encouraging.

Keywords: Digital media, illegal duplication, statistical performances, water marking, normalized cross correlation.

1. INTRODUCTION

Everyday tons of data is embedded on digital media or distributed over the internet. The data so distributed can easily be replicated without error, putting the rights of their owners at risk. Even when encrypted for distribution, data can easily be decrypted and copied. One way to discourage illegal duplication is to insert information known as watermark, into potentially vulnerable data in such a way that it is impossible to separate the watermark from the data. These challenges motivated researchers to carry out intense research in the field of watermarking.

A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. Digital watermarking is an extension of the same concept. There are two types of watermarks: visible watermark and invisible watermark. In this project we have concentrated on implementing watermark in image. The main consideration for any watermarking scheme is its robustness to various attacks. Watermarking dependency on the original image increases its robustness but at the same time we need to make sure that the watermark is imperceptible. In this project an invisible watermarking technique (least significant bit) and a visible watermarking technique is implemented. An attack is also implemented on the visible watermarked image by adding a random noise to the watermarked image. The watermarked image is then compressed and decompressed using JPEG compression finally noise is removed and the images are separated from the recovered watermarked image.

The history of watermark dates back to the 13th century. Its found as a derivative of steganography. Watermarks were used to indicate the paper brand and the mill that produced it in Italy. By the 18th century watermarks began to be used as anti-counterfeiting measures on money and other documents and in 1995 interest in digital watermarking began to mushroom. Intense research has been carried out in this field for the past few years which has led to the discovery of various algorithms [1] [2] [3] [4] [5]. Throughout this report some of these techniques are discussed and one such technique is implemented. As many advances are made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods are designed to offer better security than what cryptography can offer.

This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Watermarking is closely related to steganography, but watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication. The technique in the question is useful for copy right protection, authentication[2], broad cast monitoring and digital finger printing[3], content labeling etc.,

2. THEORETICAL BACK GROUND

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. Water marking is a subclass of steganography[1]. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. Figure 1 shows the basic block diagram of watermarking process. In the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

figure, Water marked image I_M and Attack (W) should be understood as that of functions of variables x and y. The image is taken of a local building at our college premises. The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark. Transparancy, robustness and capacity are the requirements of water marking. Out of visible, invisible, robust, public and private water marks, the Fig.1 shows the water mark shown is of public type. However, in the process after insertion, it will not be visible in the image that follows after block of water marking insertion. Out of various available schemes of water marking LSB is adapted in work of question. Its simplicity attracted as its choice in our work.

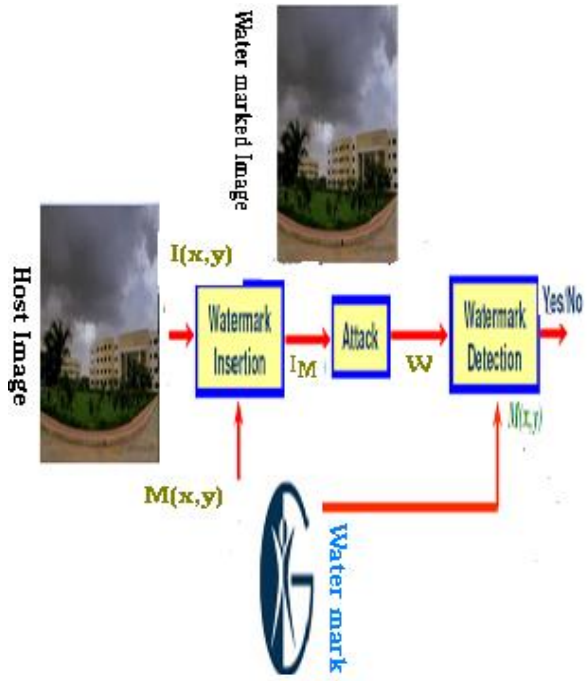

Figure 1:Block diagram

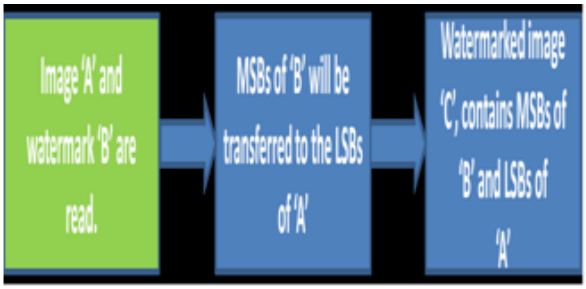

Figure2:Block diagram of adding invisible and visible water mark

3. RESULTS AND DISCUSSION

The results obtained on testing are reported in this work. Matlab algorithms were used to compute the results. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. This ratio is often used as a quality measurement between the original and a watermarked image. If one of the signals is an original signal of acceptable (or perhaps pristine) quality, and the other is a distorted version of it whose quality is being evaluated, then the MSE may also be regarded as a measure of signal quality.

MSE is a signal fidelity measure. The goal of a signal fidelity measure is to compare two signals by providing a quantitative score that describes the level of error/distortion between them. Usually, it is assumed that one of the signals is a pristine original, while the other is distorted or contaminated by errors.

Suppose that {x,y} / { x_i,y_i|i Є N, } are two finite-length, discrete signals (e.g., visual images), where N is the number of signal samples (pixels, if the signals are images) and xi and yi are the values of the i th samples in x and y, respectively. The Є in above denotes a modern algebra symbol stands for belongs to The MSE between the signals x and y is

$$MSE(\mathbf{x},\mathbf{y}) = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \quad (1)$$

Є In the MSE, we will often refer to the error signal (e_i), which is the difference between the original(x_i) and distorted(y_i) signals. If one of the signals is an original signal of acceptable (or perhaps pristine) quality, and the other is a distorted version of it whose quality is being evaluated, then the MSE may also be regarded as a measure of signal quality. MSE is often converted into a peak-to-peak signal-to-noise ratio (PSNR) measure

$$PSNR = 10\log_{10}\frac{L^2}{MSE} \quad (2)$$

Where L is the dynamic range of allowable image pixel intensities. For example, for images that have allocations of 8 bits/pixel of gray-scale, L = $2^8 - 1 = 255$. The PSNR is useful if images having different dynamic ranges are being compared, but otherwise contains no new information relative to the MSE.

The Fig.1 shows various images, WI, upon which the algorithm was implemented and their corresponding watermarked copy WM. Values for mean square error (MSE) and peak signal to noise ratio (PSNR) are measured. In Tab.1, Two images were taken. Image A, not listed, is represented by bld.jpg common for all the cases. 7 bits of watermarked img. Jpg is listed. . The normalized form of cross correlation preferred for feature matching applications. However, these must not have a simple frequency domain expression [10] Third column of Tab.1 is Normalized Cross Correlation (NCC).. This is obtained

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

from a Mat lab algorithm drafted from [10,11], that in general computes the normalized cross-correlation of matrices TEMPLATE and A. The resulting matrix C contains correlation coefficients and its values may range from -1.0 to 1.0.

Table1: VISIBLE WATERMARKING

Watermark bit no	PSNR	MSE	(NCC)
0	52.1563	0.3958	0.9995
1	50.7562	0.5463	0.9994
2	48.4209	0.9354	0.9993
3	43.3336	3.0180	0.9969
4	37.4101	11.8052	0.9782
5	32.5419	36.2150	0.952
6	31.0940	50.5453	0.840
7	29.3523	75.4831	0.595

Similar tables were estimated for invisible marking for different images, Gaussian Noise for visible marking, Salt and pepper noise visible water marking images. Similar treatment is also done for invisible water marking images.

4. CONCLUSIONS

Thus, using Matlab, two forms of watermarking techniques are implemented. One being invisible and the other being visible. Noise is added to the images as a form of attack. The noise is later removed and the watermark image is separated from the watermarked image. Finally, Quality ratio is calculated for original and watermarked image is done by PSNR, MSE and NCC values.

Appendix A

The tool used for the execution of this algorithm was 'Matlab'. The aim of the program is to replace the LSB of the base image with the MSB of the watermark. First, the program asks the user for the images to be read. The user will then enter the name of the images, both the base and the watermark, with their extension. Both these images will be read and stored by the tool, which is 'Mat lab' in our case. The tool will also display these images to the user with their respective titles. The program will then change the image size to double. This is done so as inform the tool to provide double data-type space for the images. The reason for doing so, is to provide decimal storage for the subsequent additional operations which will be performed on the base and watermark image. The next step is to assign the number of most significant bits of the watermark which will be used to overwrite on the least significant bit spaces of the base signal. Once the user provides this, the watermark signal bits are shifted to the right by the specified bits.

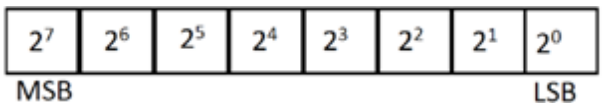

Figure 3: Representation of base image

Above represents a 8 bit image. Every pixel is represented by one 8 bit byte. Considering 3 bits in the algorithm, Whole frame is moved by 5 bits (8-3) right side, Thus pushing MSB towards LSB.

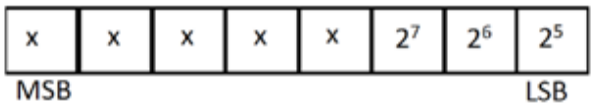

Figure4: Result after applying algorithm for 3 bits.(Watermarked image)

An exact number of these bits will be made zero in LSB of the base image. This is to provide space to store the water mark. As Fig3, base image representations is shown, it is not repeated again.

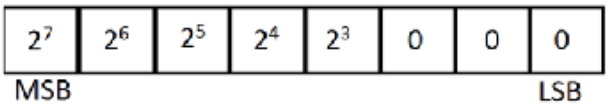

Figure5. Result after making 3zeros in LSB.

The bits of both the images, water mark image, Where MSB bits are shifted to LSB, and above image where LSB bits were made zero are added. That results water marked signal. Thus, above has 5 bits of Fig1 and 3 bits of water marked image.

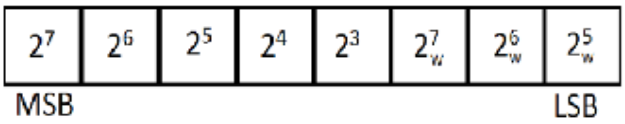

Figure6: Representation of water marked image.

REFERENCES

[1] G. K. Wallace, "The JPEG still picture compression standard", IEEE Trans. on Consumer Electronics, Vol. 38, pp.18-34, Feb. 1992.
[2] R. Popa, "An analysis of steganographic techniques", The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, 1998.
[3] P. Vidyasagar, S. Han and E. Chang. "A survey of digital image watermarking techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN 2005), edited by T. Dillon, X. Yu. and E. Chang, pp. 495-502, Perth, Western Australia, 2005.
[4] J. Dugelay and S. Roche, "A Survey of Current Watermarking Techniques" in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al, Eds. Northwood, MA: Artec House, pp. 121-145, Dec. 1999.
[5] J. Cox, et al, "Digital watermarking and steganography" (Second Edition), Morgan Kaufmann, 2008.
[6] K. R. Rao and P. Yip, "Discrete Cosine Transform: Properties, Algorithms, Advantages, Applications", Academic Press, Massachusetts, 1990.
[7] Khan and A.M. Mirza, "Genetic perceptual shaping: utilizing cover image and conceivable attack information during watermark embedding". Inf. Fusion, Vol. 8, pp. 354-365, Oct. 2007.
[8] T. C. Lin and C. M. Lin, "Wavelet based copyright protection scheme for digital images based on local features", Information Sciences: an International Journal, Vol. 17, No.9, Sept. 2009.
[9] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform", IEEE Trans. Computers, Vol. 23, pp. 90-93, Jan. 1974.
[10] P.Lewis, "Fast normalized cross correlation system", Vision Interface, 1995.
[11] J.P. Lewis, "Fast Template Matching," Vision Interface 95, Canadian Image Processing and Pattern Recognition Society, Quebec City, Canada, , p. 120-123, May 15-19, 1995