IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 12, December 2015

LSB Modification, Correlation, Transform based Digital Image Watermarking Techniques

S.A. Varaprasad[1], Palli Srinivas[2], T. Vidya[3], Ch. Aruna kumari[4]

Asst Prof, ECE Department, B.V.C College of Engineering[1, 4]

Assoc Prof, ECE Department, B.V.C College of Engineering[2, 3]

Abstract: Digital Image Watermarking, in recent times has seen a huge surge of professional work due to the skyrocketing usage of digital media. In this paper we present a competitive survey of existing watermarking techniques. This paper surveys the features and concepts pertaining to the two popular watermarking algorithm types and analyzes them to evaluate with metrics such as Time complexity, PSNR values and similarity measure of watermarks based on implementation i.e. A) Spatial based techniques (under which we analyzes LSB modification, correlation based and CDMA based techniques) and b) Transform based techniques (DCT and DWT based techniques).We have also studied the effects of different types of noises on each method.

Keywords: Image Watermarking, LSB, correlation, CDMA, DCT, DWT.

I. INTRODUCTION

Due to the exponential growth of digital media in recent years, watermarking has found its importance in almost every aspect of digital form. With its area of application coexisting in all three forms of media, i.e., image, music and video, the process of watermarking is as widespread as any digital media. Watermarking can be defined as the practice of perceptibly or imperceptibly altering a given work to embed a message about that work. Work here can be any song, video or picture. [1] Watermarking can be easily confused with a very closely related term steganography. The only thing that differentiates them is the message which we want to embed. If the message is related to the original work and it merely act as a catalyst to enhance the value of original work (the original work is given the importance) then the process of embedding is called Watermarking. On the other hand, if the message to be embedded is a secret message which may or may not be related to the original work (here the message is given the importance), then the process is Steganography. Watermarking has varied applications such as: broadcast monitoring, owner identification, proof of ownership, transaction tracking, authentication, copy control, device control, and legacy enhancements. Following are some properties of the watermarking systems. Based on these properties overall efficiency of a watermarking technique can be judged.

Watermarking Requirements:

• **Imperceptibility** the modifications caused by watermark embedding should be below the perceptible threshold.
• **Robustness** The ability of the watermark to resist distortion introduced by standard or malicious data processing.
• **Security** a watermark is secure if knowing the algorithms for embedding and extracting does not help unauthorized party to detect or remove the watermark Payload
• **Fidelity** Perceptual similarity between the original and the watermarked versions of the cover work.
• **Data Payload** No. of bits a watermark encodes within a unit of time or within a work.
• **Robustness** Ability to detect the watermark after common signal processing operations.
• **Security** The embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector (except a secret key), and the knowledge of at least one carrier with hidden message. [1]

Basically there are two main types of watermarks that can be embedded within an image.

A. Pseudo-Random Gaussian Sequence
A Gaussian sequence watermark is a sequence of numbers comprising 1 and -1 and which has equal number of 1's and - 1's is termed as a watermark. It is termed as a watermark with zero mean and one variation.

Binary Image or Grey Scale Image Watermarks

Some watermarking algorithms embed meaningful data in form of a logo image instead of a pseudo-random Gaussian sequence. Such watermarks are termed as binary image watermarks or grey scale watermarks. [7] In this paper we have obtained the results using both the possibilities of the channel being ideal and noisy.

The noises which we are applying here are Cropping, Gaussian, Poisson, Salt and Pepper, Rotational and Multiplicative noise. Images can be represented in two ways: Spatial domain and Transform domain. Spatial domain means image is represented in its pixel form, while transform domain means an image is dissected in multiple frequency bands. Each type of representation has its respective modes of watermarking techniques.

II. SPATIAL DOMAIN

Simple watermarks could be embedded in the spatial domain of images by modifying the pixel values of the image. There are mainly three types:

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 12, December 2015

A. LSB Modification

The most straight-forward method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object. As each pixel is accessible, we can embed a smaller object multiple times to tackle the problem of cropping. Due to the simplicity of this method it embarks several drawbacks in the watermarked image such as if all the LSBs of the image are set to 1, then the watermark will be completely lost. Also it is prone to many intermediate attacks like any addition of noise or lossy compression. A more reliable method will be to use a pseudo-random sequence generator to determine the pixels to be used for embedding based on a given "seed" or key. Security of the watermark would be improved as the watermark could no longer be easily viewed by intermediate parties. [16]

B. Correlation-Based Techniques

Another technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image. A pseudo-random noise (PN) pattern W(x,y) is added to the cover image I(x,y), according to the equation shown below.

$$Iw\ x, y = I\ x, y + k * W(x, y) \quad (1)$$

In above equation, k denotes a gain factor, and IW the resulting watermarked image. Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image.

To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block.

C. CDMA-Based Techniques

In the spatial domain, we can employ CDMA spread-spectrum techniques to scatter each of the bits randomly throughout the cover image, increasing capacity and improving resistance to cropping. The watermark is first formatted as a long string rather than a 2D image. For each value of the watermark, a PN sequence is generated using an independent seed. These seeds could either be stored, or themselves generated through PN methods. The summation of all of these PN sequences represents the watermark, which is then scaled and added to the cover image. To detect the watermark, each seed is used to generate its PN sequence, which is then correlated with the entire image. If the correlation is high, that bit in the watermark is set to "1", otherwise a "0". The process is then repeated for all the values of the watermark. CDMA improves on the robustness of the watermark significantly, but requires several orders more of calculation. [4]

TRANSFORM DOMAIN

In simple terms transform domain means the image is segmented into multiple frequency bands. To transfer an image to its frequency representation we can use several reversible transform like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT).

Each of these transforms has its own characteristics and represents the image in different ways.[7]

D. Discrete Cosine Transform

DCT domain watermarking can be classified into Global DCT watermarking and BlockbasedDCT watermarking. DCT is especially used for lossy data compression, because it has a strong "energy compaction" property.

One of the first algorithms presented used global DCT approach to embed a robust watermark in the perceptually significant portion of the Human Visual System (HVS). Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image.

In spatial domain it represents the LSB however in the frequency domain it represents the high frequency components.

E. Discrete Wavelet Transform

The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Wavelet Transform is computationally efficient and can be implemented by using simple filter convolution. The DWT analyzes the signal at different frequency bands with different resolutions by decomposing the signal into a coarse approximation and detail information. DWT employs two sets of functions, called scaling functions and wavelet functions, which are associated with low pass and highpass filters, respectively. The decomposition of the signal into different frequency bands is simply obtained by successive highpass and lowpass filtering of the time domain signal. The original signal x[n] is first passed through a halfbandhighpass filter g[n] and a lowpass filter h[n]. whereyhigh[k] and ylow[k] are the outputs of the highpass and lowpass filters, respectively.[19]

Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, HL).The larger the magnitude of the wavelet coefficient the more significant it is. Watermark detection at lower resolutions is computationally effective because at every successive resolution level there are few frequency bands involved. Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution.DWT is comparatively more computationally complex than DCT. [7]

III. IMPLEMENTATIONAND RESULTS

In the figure below we have shown the image results of DWT-based watermarking technique. Similar results are observed in other mentioned techniques and the difference between the results is quiet imperceptible to human eye.

In real life the channel is not ideal i.e. the channel is not noiseless. When the images are transmitted from one place to another, the images get distorted due to the presence of noise in the channel.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 12, December 2015

Figure 1(a): Original

Figure 1(b): Watermark

Figure 1(c): Watermarked Image

Figure 1(d): Recovered Watermark

Table 1: Comparison of different techniques

Technique	Processing time (sec)		PSNR (dB)
	Embedding	Recovery	
LSB Substitution	1.7820	0.3910	50.868
Correlation Based	0.7810	0.4380	54.9790
CDMA	3.7650	4.6250	31.0350
DCT Based	2.0930	0.7340	33.8132
DWT Based	11.4220	18.1090	41.5961

Based on the above table we have plotted a comparative graph for better understanding.
The watermarked image gets distorted due to the noise present in the transmission channel. So here we have shown the effects of some noises and distortions on the watermarked image and the watermark extracted from this noisy/distorted watermarked image.

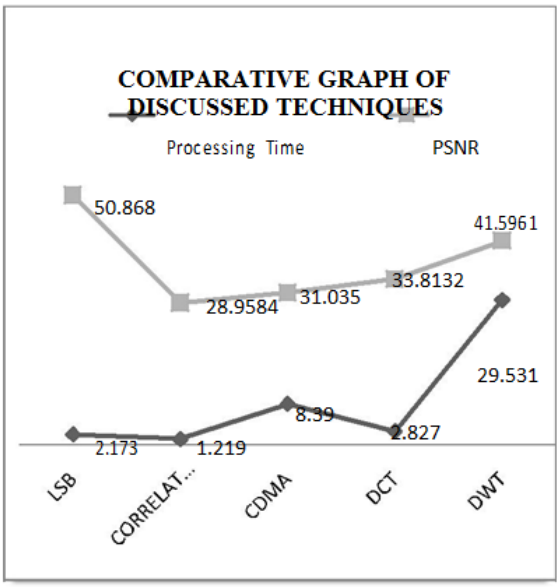

Figure2: Comparative Graph of Discussed Techniques

Below we have enlisted a table which compares all the discussed methods based on their respective processing time and PSNR values when subjected to different attacks at the time of recovery.

The PSNR values have no direct relation with the visual quality of the image. An image with good PSNR can have low visual quality and vice versa.

Since, PSNR is not an efficient comparison tool, so we have compared every pixel of the original watermark with the recovered watermark and enlisted our results in the below table. The results are in the form of percentage similarity between recovered watermark and original watermark.

Techniques	Attacks	Processing time (sec)	PSNR (dB)
LSB substitution	Cropping	0.2970	12.8542
	Gaussian noise	0.6720	19.7732
	Poisson	0.7970	26.8527
	Rotation	1.4530	9.5756
	Salt and pepper	0.6720	18.1240
	Multiplicative	0.6560	19.4192
Correlation based	Cropping	0.8280	12.9359
	Gaussian noise	0.9060	19.7445
	Poisson	1.0620	26.7967
	Rotation	3.6250	9.5752
	Salt and pepper	0.9070	18.2771
	Multiplicative	0.9060	19.4522
CDMA	Cropping	0.6720	12.7818
	Gaussian noise	5.3440	18.5951
	Poisson	5.5000	25.4715
	Rotation	10.5160	7.6107
	Salt and pepper	5.4220	17.3181
	Multiplicative	5.3440	19.1694
DCT based	Cropping	3.2350	12.3552
	Gaussian noise	3.2650	11.3432
	Poisson	3.4370	25.8546
	Rotation	20.2500	9.5664
	Salt and pepper	3.3440	18.1374
	Multiplicative	3.3600	19.2677
DWT based	Cropping	18.5780	12.2731
	Gaussian noise	18.2340	19.1264
	Poisson	18.4380	26.7330
	Rotation	18.6400	9.5749
	Salt and pepper	18.2660	17.6891
	Multiplicative	18.2030	19.4113

Table 2: Comparison of different techniques under attacks

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 12, December 2015

Table 3: Similarity analysis of recovered watermark with original watermark

Techniques	Attacks	Similarity measure of watermarks (%)
LSB substitution	Cropping	82.6000
	Gaussian noise	48.3000
	Poisson	49.6000
	Rotation	40.9000
	Salt and pepper	81.6000
	Multiplicative	49.4000
Correlation based	Cropping	48.5000
	Gaussian noise	55.6000
	Poisson	60.3000
	Rotation	44.6000
	Salt and pepper	53.3000
	Multiplicative	53.7000
CDMA	Cropping	50.9000
	Gaussian noise	92.7000
	Poisson	95.5000
	Rotation	49.8000
	Salt and pepper	92.1000
	Multiplicative	93.6000
DCT based	Cropping	51.1000
	Gaussian noise	94.5000
	Poisson	99.8000
	Rotation	63.1000
	Salt and pepper	86.6000
	Multiplicative	88.7000
DWT based	Cropping	50
	Gaussian noise	96.5000
	Poisson	99.6000
	Rotation	49.5000
	Salt and pepper	94.1000
	Multiplicative	96.7000

IV. CONCLUSION

This study has introduced a number of techniques for the watermarking of digital images, as well as touching on the limitations and possibilities of each. Although only the very surface of the field was scratched, it was still enough to draw several conclusions about digital watermarking.

LSB substitution is not a very good candidate for digital watermarking due to its lack of even a minimal level of robustness. LSB embedded watermarks can easily be removed using techniques that do not visually degrade the image to the point of being noticeable.

Another observation is that transform domains are typically better candidates for watermarking then spatial, for both reasons of robustness as well as visual impact. By anticipating which coefficients would be modified by the subsequent transform and quantization, we were able to produce a watermarking technique with moderate robustness, good capacity, and low visual impact.

The wavelet domain as well proved to be highly resistant to noise, with minimal amounts of pixel degradation, this is shown in table 3 as we have found that recovered watermark is more similar to original watermark in wavelet domain method Here we have applied a considerable amount of noise to view a significant distortion in the image. The wavelet domain may be one of the most promising domains for digital watermarking yet found. But a natural find is that none of the above techniques are completely robust to the geometric distortions.

V. FUTURESCOPE

Although none of the technique is completely robust to all the distortions, still techniques can be tabulated where in they are robust to few categories of attacks. Also we are working in the area of Reversible watermarking where high embedding capacity and good PSNR is a matter of concern. The results of our work will be published shortly.

REFERENCES

[1]. Cox IJ, Miller ML & Bloom, JA 2002, "Digital Watermarking andSteganography", Morgan Kaufmann Publisher, San Francisco, CA, USA.
[2]. Gonzalez and Woods, "Digital Image Processing", PHI ,Second Edition, 2005.
[3]. Arthur Weeks Jr., "Fundamentals of Digital Image Processing", Eastern Economy Edittion, 2005.
[4]. T. Ramashri and S. Narayana Reddy, "Robust Image Watermarking Algorithm Using Decimal Sequences", International Journal of WirelessNetworks and Communications Volume 1, Number 1, pp. 1–8, 2009.
[5]. Suhad Hajjara, Moussa Abdallah & Amjad Hudaib, "Digital Image Watermarking Using Localized Biorthogonal Wavelets", European Journal of Scientific Research ISSN 1450-216X Vol.26 No.4 , pp.594-608, 2009.
[6]. T. Furon_ and P. Duhamel, "An Asymmetric Watermarking Method", IEEE Transaction On Signal Processing, Vol. 51, No. 4, April 2003
[7]. Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", Proc. IEEE Int. Conf. On IndustrialInformatics (INDIN), 2005.
[8]. MahaSharkas, Dahlia ElShafie, and NadderHamdy," A Dual Digital-Image Watermarking Technique", World Academy of Science,Engineering and Technology , 2005
[9]. Mei Jiansheng, Li Sukang1 and Tan Xiaomei, "A Digital Watermarking Algorithm Based On DCT and DWT", Proceedings of the InternationalSymposium on Web Information Systems and Applications, 2009
[10]. Peining Tao and Ahmet M. Eskicioglu, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain", Internet multimedia management systems V (Philadelphia PA, 26-28 October 2004)
[11]. Nitesh Dixit and AnkushAgarwal, "Wavelets based Digital Watermarking", March 2004.
[12]. Ingemar J. Cox and Matt L. Miller, "Electronic Watermarking: The First50 Years", Published in the Proceedings of the IEEE 2001 Int. Workshop on MultiMedia Signal Processing, 2001.
[13]. Van Schyndel, R.J., Tirkel, A.Z., Osborne, A.F., "A digital watermark,"Proc.IEEE Int. Conf. Image Processing, vol. 2, 86-90, 1994
[14]. PeiningTaoa and Ahmet M. Eskicioglub, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain", The Graduate Center, The City University of New York, 365 Fifth Avenue, New York, NY 10016 Department of Computer and Information Science, Brooklyn College, The City University of New York, 2900 Bedford Avenue, Brooklyn, NY 11210.
[15]. Kamran Hameed, AdeelMumtaz, and S.AM. Gilani, "Digital Image Watermarking in the Wavelet Transform Domain", World Academy of Science,EngineeringandTechnology,13,2006
[16]. M. S. Sutaone , M.V. Khandare "Image Based Steganography Using LSB Insertion Technique", IEEE WMMN pp. 146-151, January 2008.
[17]. Gerhard C. Langelaar, IwanSetyawan, and Reginald L. Lagendijk "Watermarking Digital Image and Video data", in Proc. IEEE Int. Conf. A State-of-the-Art Overview, September 2000.
[18]. DeepaKundur and DimitriosHatzinakos,"Digital Watermarking Using Multiresolution Wavelet Decomposition", In Proc. IEEE Int. Conf., 1998
[19]. http://www.rowan.edu/wavelet
[20].https://www.digimarc.com/resources/docs/DMRC_WatermarkingGuide. pdf