

Image Authentication Using Digital Watermarking

Dr. Bhupesh Kumar Singh¹, Tanu Dua²

^{1,2}Department of Computer Science & Engineering, RAWAL Institute of Engineering & Technology, Faridabad, India

ABSTRACT:

Watermarking is a technology used to embed some kind of information inside a digital content (text, image, audio or video) using different techniques. The embedded information depends upon the application. Watermark should be robust and imperceptible. Robustness of watermark can be explained in terms of successful recovery of watermark from recovered content which may contain different types of noises and compression effects. After recovering the watermark, the recovered and original watermarks are compared by calculating of similarity factor (SMF) of these two watermarks. If the similarity factor is closer to one than we can conclude that the content is original and/or authenticated. This paper entails the study of watermarking technique and delve deeper to improve the robustness of the image. To achieve this, a detailed insight is provided into few techniques explaining each one as a comprehensive step by step procedure and calculating SMF and Peak signal to Noise ratio (PSNR) for different samples considering various attacks.

Keywords: Authentication, Watermarking, Discrete Cosine Transform, Noise Attacks, Similarity Factor, Peak Signal to Noise Ratio.

I. INTRODUCTION

Image Authentication is the application of image processing and domain expertise to discern if a questioned image or video is an accurate representation of the original data by some defined criteria. The digital communication technology (internet) confronts various troubles related to the privacy and security of the data. Security techniques are required because of unauthorized access of data without permission. So, it is necessary to protect data on the internet. For providing the security of digital data various techniques are used like encryption, decryption, cryptography, steganography and digital watermarking. A Digital Watermark is used to communicate copyright information about an image in order to reduce copyright infringement. A person opening a digitally watermarked image in an image editing application or our Internet- or Windows-Explorer reader receives notification through a copyright symbol ((c)) that the image contains copyright and ownership information. The digital watermark can provide a link to complete contact details for the copyright holder or image distributor, making it easy for the viewer to license the image, another one like it, or commission new work. Digital watermarks are added to digital images in a way that can be seen by a computer but is imperceptible to the human eye; yet provide images with a durable, persistent identity. A digital watermark carries a message containing information about the creator or distributor of the image, or even about the image itself. We vary the digital watermark energy to help hide the digital watermarks within the image so that it remains imperceptible. The digital watermark is robust, surviving many typical image edits and file format conversions.

II. RELATED WORK

Watermark is basically categorized in two categories on the basis of processing, namely,

- Spatial Domain
- Transform Domain

2.1 Spatial Domain Techniques

Spatial Domain approaches use the minor changes in the pixel value intensity. The simplest example of the former techniques is to embed the watermark in the least significant bits of image pixels. In other words, significant portions of low frequency components of images should be modified in order to insert the watermark data in a reliable and robust way. For instance, an image is divided into the same size of blocks and a certain watermark data is added with the sub-blocks. In this technique, watermark is embedded by directly amending

the pixel values of the host image/video. The foremost advantages of pixel based methods are that they are conceptually simple having very low computational intricacies. These methods are, therefore, commonly used in video watermarking where the prime concern is real-time performance [2]. Methods of watermarking in spatial domains are namely:

- Correlation based Techniques
- Least Significant Bit Modification (LSB)

2.1.1 Correlation based Techniques:

In this technique, the watermark $W(x, y)$ is added to the original content $O(x, y)$ according to the equation.

$$O_w(x, y) = O(x, y) + kW(x, y)$$

where, k is a gain factor and O_w is the watermarked content. As we increase the value of k , it will expense the quality of watermarked contents.

2.1.2 Least Significant Bit Modification (LSB):

Least Significant Bit modification (LSB) is the simplest technique of this domain. In this method, the watermark is just embedded into the least significant bits of the original video or flips the LSB. Though it is the most popular scheme due to its simplicity, but has some limitations like incompetence in dealing with a range of attacks, poor quality of the produced video, least robustness and lack of imperceptibility [3]. In this technique the third and the fourth least significant bits are used for the insertion of watermark. This technique is more robust than the traditional LSB technique for insertion of digital watermark and quality of the watermarked image is also higher [4]. A 12 bit watermark is created from each block of the host image in this technique and the watermark is embedded in the last 3 significant bits of each block. This technique is efficient for tamper detection in images [5]. Generalized patchwork algorithm is an extension of the modified patchwork algorithm (MPA). The MPA inserts the watermark into the image additively and changes the mean of the pixels accordingly. The GPA combines both additive watermarks and multiplicative watermarks. The embedding functions of the GPA determine the embedding parameters adaptively according to the host signals. Detection functions of GPA also determine threshold adaptively. The advantage of GPA is that it is sufficiently robust against various signal processing operations specially against compression attacks [6].

2.2 Transform Domain Techniques

Transform domain is also called frequency domain because values of frequency can be altered from their original. In this method, transform coefficients are modified for embedding the watermark. The most important techniques in transform domain are discrete cosine transform (DCT) and Discrete Wavelet Transform (DWT). This watermarking algorithm is based on image segmentation and Discrete Cosine Transform (DCT). The image is first segmented using Expectation Maximization (EM) into blocks of size 8 by 8 pixels. The DCT of each block is computed then. After that a pseudorandom sequence of real numbers is embedded in the DCT domain of each block of image. This technique is robust to common signal distortions including geometric manipulation [7]. This digital image watermarking technique is based on discrete cosine transform (DCT) and neural network. The neural network is full counter propagation neural network (FCNN). FCNN has been used to simulate the perceptual and visual characteristics of the original image. The perceptual features of the original image have been used to determine the highest changeable threshold values of DCT coefficients. The highest changeable threshold values have been used to embed the watermark in DCT coefficients of the original image. The watermark is a binary image. The pixel values of this image are inserted as zero and one values in the DCT coefficients of the image [8]. This technique of watermarking is based on the Quadratic DCT transform. This technique firstly performs block DCT transform on the host image and selects the transformed DC coefficients in each block to form a new matrix. It then conducts another block DCT transform on the new matrix. The high frequency coefficients of DCT coefficients are selected to embed the watermark. For extracting the watermark this technique does not need original image thus achieves the blind detection. This technique has good imperceptibility and is robust against filtering, noise and other attacks [9]. This technique combines FABEMD and DCT to insert watermark in images. The FABEMD decomposition is a method based on decomposing an image into multiple hierarchical components known as Bidimensional Intrinsic Mode Functions (BIMFs) and residue. In the traditional DCT based methods the watermark is embedded directly in the DCT coefficients of the host image. In this technique the watermark is embedded in the DCT coefficients of the residue which makes it more robust and perceptually invisible compared to traditional DCT based watermarking techniques [10].

III. WATERMARKING AND ITS TYPES

There are different classifications of digital watermark algorithms as discussed in [1]. Watermark techniques can be broadly categorised into four different clusters:

3.1 According to type of data to be watermarked

- Text watermarking
- Image watermarking
- Video watermarking
- Audio watermarking

3.2 Based on human perception

- Visible watermarking
- Invisible watermarking

Visibility is associated with perception of the human eye so that if the watermark is embedded in the data in the way that can be seen without extraction, we call the watermark visible. Examples of visible watermarks are logos that are used in papers and video. On the other hand, an invisible watermarking cannot be seen by human eye. So it is embedded in the data without affecting the content and can be extracted by the owner or the person who has right for that. For instance images distribute over the internet and watermarked invisible for copy protection.

3.3 Based on information for detection

- Blind or public watermarking: In public watermarking, there is no need for original signal during the detection processing to detect the watermark. Only the secret key is required. For example, in image blind watermarking we do not need the original image.
- Non-blind or private watermarking: In non-blind or private watermark, original signal is required for detection the watermark.
- Semi-blind watermarking: In semi-blind watermarking, sometimes we may need some extra information for detecting the watermark. Some watermarking techniques require access to the original signal just after adding the watermarking, which is called published watermarked signal. This form of watermarking is called semi-blind watermarking.

3.4 Based on processing-domain

- Spatial domain: A watermark technique based on the spatial domain, spread watermark data to be embedded in the pixel value.
- Transform domain: To have imperceptibility as well as robustness, adding of watermark is done in transform domain.

In addition to above, watermark technique can also be classified on the robustness feature.

- Robust watermark: One of the properties of the digital watermarking is robustness. We call a watermark algorithm robust if it can survive after common signal processing operations such as filtering and lossy compression.
- Fragile watermark: A fragile watermark should be able to be detected after any change in signal and also possible to identify the signal before modification. This kind of watermark is used more for the verification or authenticity of original content.
- Semi-fragile watermark: Semi-fragile watermark is sensitive to some degree of the change to a watermarked image.

Furthermore, from application point of view, watermark techniques can be grouped as source based or destination based.

In source based, all copies of a particular data have a unique watermark, which identifies the owner of that data, while in the destination based; each distributed copy is embedded using a unique watermark data, which identifies a particular destination.

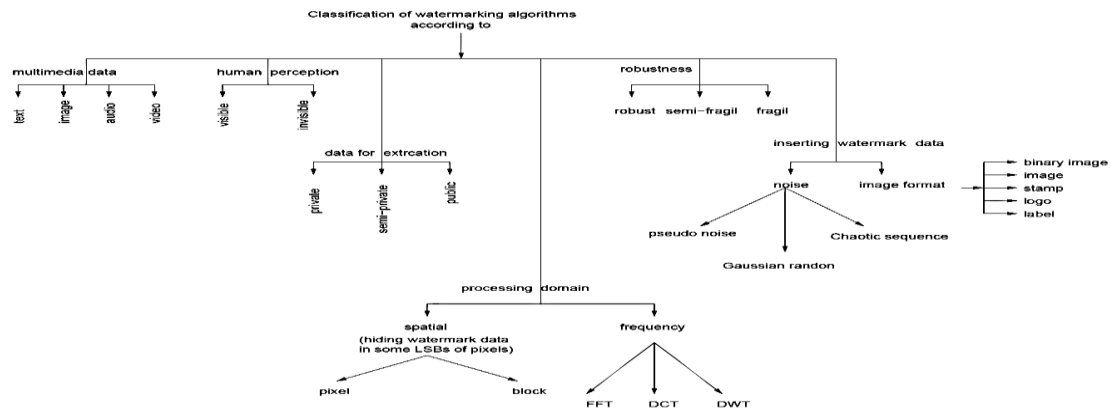


Figure 1: Classification of Digital Watermarking.

IV. PROPOSED METHOD

As the objective is to analyse the robustness of watermarking techniques spatial domain techniques are not considered here, only temporal domain techniques are considered. The DCT technique is used for the implementation. The input RGB image is converted into is gray scale image is decomposed into 8x8 blocks by the 2D DCT which creates low energy matrix coefficients of HL plane. According to the pattern of the randomized watermark image, for each block a variation among the column coefficients is generated. The modified coefficients are once again merged with the unaffected bands to get the watermarked image as discussed in Figure2.

Steps for the proposed method as follows:

1. Input image [MXN].
 - 1.1 If the image is coloured then convert it into gray scale images
2. Segment the image [MXN] into [8x8] blocks for processing.
3. Apply forward DCT to each of these blocks .
4. Apply block selection method.
5. Modify the selected co-efficient and Embedd watermark.
6. Apply inverse DCT transform on each block [8x8].

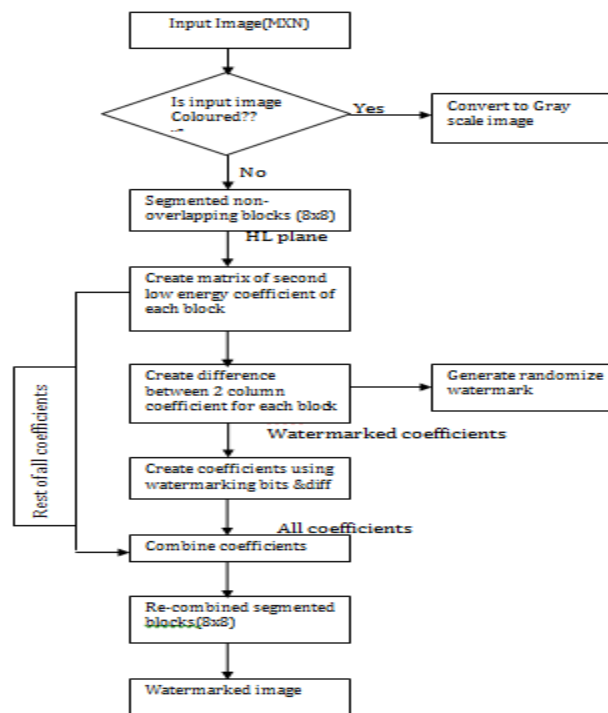


Figure 2: Proposed System

A watermarked image is decomposed into 8x8 block coefficients using DCT. The HL plane coefficients thus created are used to derive the watermarking bits with the help of difference in the coefficients. Now the extracted water mark can be used to find out the similarity factor and the PSNR.

4.1 Advantages of DCT

1. DCT is better than any of the spatial domain techniques because it is robust against various kinds of attacks like cropping, noising, filtering and sharpening.
2. DCT is a real transform with better computational efficiency.
3. The DCT gives a better performance in the bit rate reduction.
4. DCT also implements fast algorithms. [11]

4.2 Effect of Noise attacks on Watermarks

The effect of various types of noise on the robustness of watermarks is analyzed. Following types of noise are considered

1. Salt and pepper noise: It is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels. An effective noise reduction method for this type of noise involves the usage of a median filter or a contra harmonic mean filter. Salt and pepper noise creeps into images in situations where quick transients, such as faulty switching, take place.

2. Speckle noise: It is a granular noise that inherently exists in and degrades the quality of the images. Speckle noise results from random fluctuations in the return signal from an object that is no bigger than a single image-processing element. It increases the mean gray level of a local area. Speckle noise is generally more serious, causing difficulties for image interpretation.

3. Gaussian noise: It is statistical noise that has its probability density function equal to that of the normal distribution, which is also known as the Gaussian distribution. In other words, the values that the noise can take on are Gaussian-distributed. A special case is white Gaussian noise, in which the values at any pairs of times are statistically independent (and uncorrelated). In applications, Gaussian noise is most commonly used as additive white noise to yield additive white Gaussian noise (AWGN).

There exist a number of other attacks like JPEG compression, cropping, resizing etc. that affect the quality of the watermark extracted.

The following two quality measures have been considered to evaluate the performance of digital watermarking techniques

➤ **Similarity Factor (SMF):**

For the evaluation of the whole process after the successful recovery of watermark from the watermarked content, the recovered watermark has to compare with original watermark. Similarity Factor defined as the co-relation between the original watermark (W_o) and recovered watermark (W_r) using the following equation(1). The Value of the Similarity Factor (SMF) will be between 0 and 1. The Good Result corresponds to the values closer to 1. SMF is defined as:

$$SMF = \frac{\sum_{i=1}^N W_o \times W_r}{\left(\sqrt{\sum_{i=1}^N W_o^2} \times \sqrt{\sum_{i=1}^N W_r^2} \right)} \quad (1)$$

Where, N = Total No. of Pixels in the watermark image.

➤ **Peak Signal to Noise Ratio (PSNR):**

Peak Signal to Noise Ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel scale because many signals have a very wide dynamic range. The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codec. The signal in this case is the original data, and the noise is the error introduced by compression.

The value range of PSNR will vary from types of content compared. One has to be extremely careful with the range of validity of this metric as it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content. The general accepted values are values more than 30 db. It is most easily defined via the mean squared error (MSE) with following equation(2) for two $m \times n$ images I and K where one of the images is considered a noisy approximation (here image k) of the other is defined in following equation (3).

$$MSE = (1 / n \times m) \times \sum_{i=1}^m \sum_{j=1}^n [I(i, j) - K(i, j)]^2 \tag{2}$$

$$PSNR = 20 \times \log(Im \div \sqrt{MSE}) \tag{3}$$

V. EXPERIMENTAL RESULTS

In order to test the performance of the proposed system .We have performed the experiment with five different samples and considered four different noise-attacks. We used [640x480] size standard coloured and gray scale images as a samples using MATLAB as a tool.

Samples→		Eye		Flower		Butterfly		Palm		Ship	
S.no	Attacks	SMF	PSNR	SMF	PSNR	SMF	PSNR	SMF	PSNR	SMF	PSNR
0	No-Noise	0.9979	43.3475	0.9957	46.2858	0.9869	39.8611	0.6671	41.0703	0.9992	47.9588
1	Salt&PepperNoise	0.9653	42.5401	0.9595	44.8410	0.9595	39.4963	0.6331	40.5953	0.9661	45.9281
2	Speckle Noise	0.7189	41.7554	0.8292	44.9718	0.8292	39.6244	0.3204	39.1183	0.7078	44.7784
3	Gaussian	0.4681	40.1377	0.4842	41.2880	0.4842	38.2070	0.4704	38.9440	0.4890	41.7546
4	For Add. White Gaussian Noise	0.3912	27.4958	0.4156	27.8078	0.4198	27.9331	0.3752	27.3753	0.3811	27.5452

Figure3: Observation Tables of Different Samples with SMF&PSNR



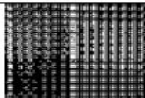















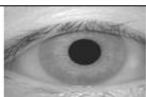

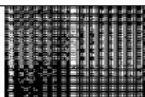
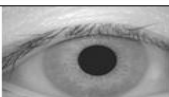




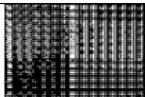



Original Image	Original Watermark	Randomize Watermark	Watermarked Image	Extracted Randomize Watermark	Extracted Original Watermark
					
					
					
					
					

Figure4: Conformance Experiment of the Watermarked Images

VII. CONCLUSION

Watermarking technique is commonly used method for providing security to digital media on the internet technology. In this paper, study of watermark technique based on domain. We discuss the limitation of different techniques. The efficiency of the proposed system is established with the help of experimental results. The proposed algorithm can be further improved using various edge detection techniques and further can be extended to video processing.

REFERENCES

- [1] Yanqu Zhang, "Digital Watermarking Technology: A Review", Future Computer and Communication, 2009. FCC '09. International Conference.
- [2] A. A. Hood and Prof. N. J. Janwe, "Robust Video Watermarking Techniques and Attacks on Watermark – A Review", *International Journal of Computer Trends and Technology*, vol. 4, Issue No. 1, pp. 30-34, 2013.
- [3] S. Patel, A. K. Katharotiya and M. Goyani, "A Survey on Digital Video Watermarking", *International Journal Comp. Tech. Appl.*, Vol. 2 (6), pp. 3015-3018, Nov. - Dec. 2011.
- [4] Bamatraf, a.; Ibrahim, R.; Salleh, M., "Digital Watermarking algorithm using LSB", Computer Applications & Industrial Electronics, (ICCAIE), 2010 International Conference on 5-8 Dec. 2010.
- [5] Dadkhah,S.; Manaf,A.; Sadighi, S., "Efficient two level image tamper detection using three LSB watermarking", Computational Intelligence and Communication Networks(CICN) 2012, Fourth International Conference.
- [6] In Kwon Yeo, HyoungJoong Kim, Multimedia Systems, "Generalized patchwork algorithm for image watermarking", Sep 2003, Volume 9, Issue 3, pp 261-265.
- [7] Badran, E.F.; Ghobashy, A.; El-Shennawy, K., "DCT-Based Digital Image Watermarking Via Image Segmentation Technique", Information and Communications Technology, 2006, ICICT'06.ITI 4th International Conference, Dec 2006.
- [8] NaghshNilchi, A.R. ; Taheri, A., "A new robust digital image watermarking technique based on the Discrete Cosine Transform and Neural Network", Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium.
- [9] Sivavenkateswara, R.V. ; Shekhawat, R.S. ; Srivastava, V.K., "A DWT-DCT-SVD based digital image watermarking scheme using particle swarm optimization", Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference.
- [10] Aherrahrou, N. ;Tairi, H., "Robust digital image watermarking based on joint FABEMD-DCT", Multimedia Computing and Systems (ICMCS), 2012 International Conference.
- [11] Preeti Parashar ; Rajeev Kumar Singh , " A Survey: Digital Image Watermarking Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014)