

MODELLING OF GEOMETRIC ATTACKS FOR DIGITAL IMAGE WATERMARKING

Vaishali Jabade

Research Student, Electronics Dept., Walchand Institute of Technology, Solapur, India

Dr. Sachin Gengaje

Head, Electronics Dept., Walchand Institute of Technology, Solapur, India

ABSTRACT

Digital media causes extensive threat in terms of piracy of copyrighted material. Consequently, watermarking has been widely studied as a component of Digital Rights Management (DRM) and protecting Intellectual Property Rights (IPR). The ways and means are required to detect copyright violations and control access to these digital media. This has stimulated the development of digital watermarking. Protecting integrity, validity and ownership of digital multimedia has become a major issue today. Reliable transmission of data over Internet and verification of originality of this data has become a challenge. This leads to the need of studying, analyzing and modelling various attacks on watermarked image. The watermarked image is often subjected to geometric transformation resulting in degradation of the quality of watermarked image. Comprehensive study and analysis of geometric attacks is carried out to study its effect on degradation of the quality of watermarked image.

KEYWORDS: Digital Image Watermarking, Geometric Attacks, Modelling, Watermarked Image.

INTRODUCTION

Digital image watermarking is represented in Fig.1. It involves embedding a pattern called as watermark W in an image I to mark ownership. The image in which watermark is to be inserted is referred to as host image, original image or cover image. The watermarked image I_w is transmitted over watermark channel where it may be subjected to different geometric attacks. The attacks modify the watermarked image resulting in a degraded image $I'w$. This watermarked image is used for extraction of the watermark embedded [1-4].

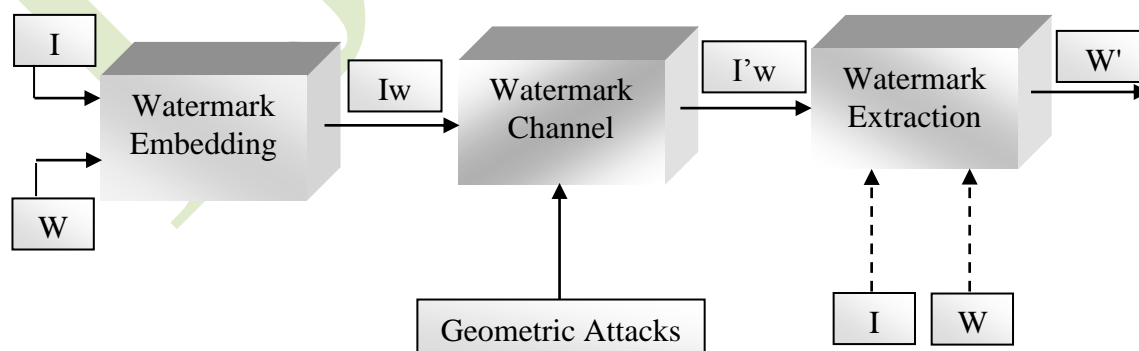


Fig. 1 Digital Watermarking Representation using Geometric Attacks

ATTACKS ON WATERMARKED IMAGE

Watermark channel introduces distortion in watermarked image and hence in embedded watermark. The watermarked image is also likely to be subjected to certain manipulations, some unintentional such as compression and transmission noise and some intentional such as cropping, filtering etc. Such distortion or manipulation is defined as attack on watermarked image [5-7].

Performance of distorted images in image watermarking is tested and judged for robustness evaluation. Robustness indicates survival of watermark in the watermarked image even if image is subjected to any distortion or manipulation. The possible attacks are broadly classified as shown in Fig. 2. These attacks are summarized below.

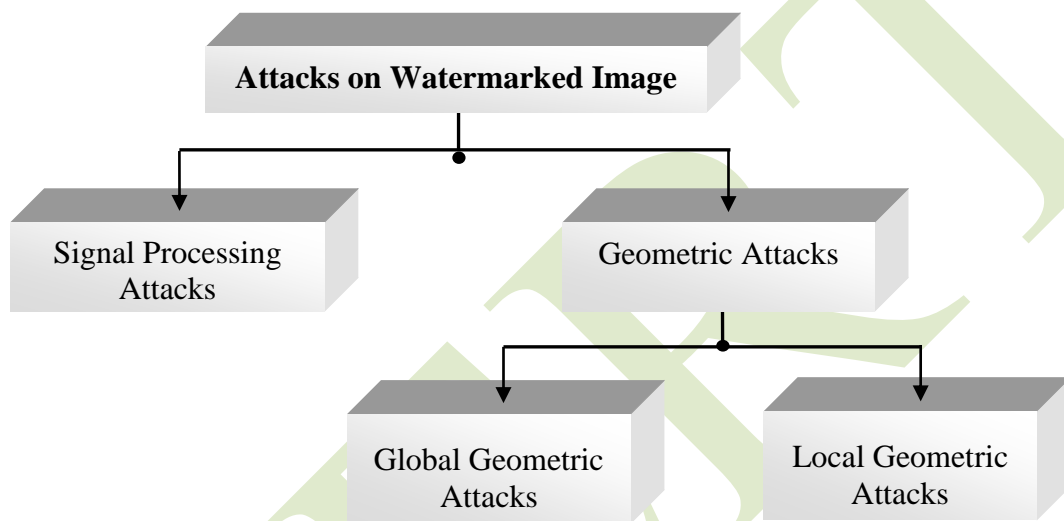


Fig. 2 Classification of Attacks on Watermarked Image

Geometric Attacks

These attacks are also called as de-synchronization attacks. Geometric attacks are geometric distortions to an image and include operations such as rotation, translation, scaling and cropping etc. Geometric attacks attempt to destroy synchronization of detection thus making detection process difficult and sometimes even impossible. The distortion due to geometric attack is clearly visible. Geometric attacks are classified basically into two types as global geometric and local geometric attacks. Global geometric attacks affect all the pixels of an image in similar manner. The examples include rotation, scaling, translation etc. Local geometric attacks affect different portions of an image in different ways. These attacks include cropping, row-column blanking, warping etc. Rotation, translation and scaling attacks are examples of affine transform. Basic transformations which come under geometric attacks are listed in table 1 [8-16].

Cropping

Cropping refers to cutting or clipping part of the watermarked image. Cropping is used for the removal of the outer or inner parts of an image to improve framing, emphasizing subject matter or changing aspect ratio. Image cropping is a widely used geometric attack on watermarked image. The process involves removal of even some watermark information along with image itself. Cropping is the easiest operation among image manipulation operations. The circumference of watermarked image is cropped from sides. Here minimum

or maximum pixel value is inserted in the cropped portion. The remaining central part of the watermarked image is used to extract watermark. Watermarked image can be cropped from borders or in middle portions.

Table 1. Types of Geometric Attacks

Sr. No.	Type of Attack	Description of Attack
1	Cropping	Cropping an image from borders or middle portion. The portion of an image may be replaced by black or white pixels. Cropping process may remove some watermark information.
2	Rotation	Rotating an image clockwise or anticlockwise by different angles.
3	Image Flipping	Flipping an image horizontally or vertically without losing any value to realign features.
4	Row-Column Blanking	Blanking different rows and columns in an image. It refers to deleting few rows and columns simultaneously. This can be achieved by replacing pixels by maximum gray level.
5	Scaling	Modifying aspect ratio of an image. It can be uniform or non-uniform.
6	Warping	Causing significant distortion of shapes portrayed in an image.
7	Translation	Repositioning an image by applying a shift along a straight line path from one coordinate location to the other co-ordinate location.
8	Local exchange of pixels	Pixel values are interchanged locally. The corresponding portions in an image are swapped.

Rotation

The watermarked image is rotated by different angles and still watermark can be extracted. Image rotation makes co-ordinate axes changed. Without synchronization to orthogonal axes, one cannot extract watermark correctly. The question of geometrically distorted axis recovery is to be considered. It is assumed that the distorted axes have been recovered before watermark is detected. The axis recovery is done for an angle of. Rotation does not destroy visual content of the image but due to rotation, some pixels move to new positions and embedded watermark can be removed. The rotation operation performs geometric transform which maps position (x_1, y_1) of an input image to a new position (x_2, y_2) by rotating an image through an angle θ about origin. Rotation operation is used for pre-processing operation and to improve visual appearance. The rotation operator performs the transformation of the form given by following equation.

$$x_2 = x_1 \cos\theta + y_1 \sin\theta \quad (1)$$

$$y_2 = -x_1 \sin\theta + y_1 \cos\theta \quad (2)$$

Where

θ : Rotation angle

(x_1, y_1) : Original co-ordinates

(x_2, y_2) : Transformed co-ordinates

Image Flipping

It is also called as mirroring an image. This is widely used form of rotating an image with fixed rotation angle theta. The modelling resembles that of rotation. The image is horizontally rotated without losing any value to realign its horizontal features. Similarly, vertical flip of an image is also possible showing similar effects.

Row-Column Blanking

This geometric operation leads to blanking of few rows and columns in a watermarked image accidentally or intentionally. The pixel values are replaced by zeros making the blanked portion in an image black. The watermarked image is subjected to blanking of some portion in an image. If equal number of rows and columns are blanked, the blanked portion appears to be a square. If unequal number of rows and columns are blanked, the blanked portion appears to be a rectangular.

Scaling

Image scaling is the process of resizing the watermarked image. Scaling modifies aspect ratio of an image. Scaling can be applied depending on the demand of storage requirement of an image. It performs geometric transformation that can compress or expand an image in size. Expansion is possible by replicating single pixel value or interpolation method. Scaling can be uniform or non-uniform. Scaling factor is same in horizontal and vertical direction under uniform scaling whereas uses different scaling factors in horizontal and vertical direction under non-uniform scaling. Scaling is a special case of affine transformation and represented mathematically as follows.

$$g_{height} = \frac{f_{height}}{f_{width}} \times g_{width} \quad (3)$$

$$g_{width} = \frac{f_{width}}{f_{height}} \times g_{height} \quad (4)$$

Where

f_{width}, f_{height} : Original scale

g_{width}, g_{height} : New scale

Warping

Warping an image is the process of digitally manipulating the watermarked image. It causes significant distortion of shapes representing the image. Warping may be used for correcting image distortion, morphing or for creativity purpose. The modelling varies depending on warping requirement.

Translation

The translation operation performs a geometric transformation which maps position of each pixel in watermarked input image to a new position in an output watermarked image. A translator shifts the watermarked image by a specified number of pixels in either x or y direction, or both. The origin of image gets shifted to a new location as shown below.

$$x_2 = x_1 + \Delta x \quad (5)$$

$$y_2 = y_1 + \Delta y \quad (6)$$

Where

(x_1, y_1) : Origin

(x_2, y_2) : Transformed origin

Δx : Shift of origin along x-direction

Δy : Shift of origin along y-direction

Local Exchange of Pixels

This is a type of geometric attack in which neighboring pixels in watermarked image get exchanged. Pixel values are interchanged locally. There is swapping of neighbourhood pixel values resulting in swapped image portions.

PERFORMANCE ANALYSIS

Performance analysis for attacked watermarked image is carried out using different statistical measures. For benchmarking and performance evaluation, visual degradation of watermarked image due to geometric attack is important. The mathematical analysis is carried out by measuring various parameters. Following metrics are used as a quantitative measure [17-20]. The notations used are listed below.

$I(x, y)$: Host image,
 $Iw'(x, y)$: Attacked Watermarked image, and
 N_t : Size of an image

Mean Square Error (MSE)

Mean Square Error is the error between host image and watermarked image and is calculated as follows. Minimum value of MSE is desirable.

$$MSE = \frac{1}{N_t} \sum_{x,y} (I(x, y) - Iw'(x, y))^2 \quad (7)$$

Peak Signal to Noise Ratio (PSNR)

Peak signal to noise ratio is widely used image quality metric and is defined in decibels as

$$PSNR(dB) = 10 \cdot \log_{10} \frac{255 \times 255}{MSE} \quad (8)$$

PSNR is calculated between host image and attacked watermarked image. It is measured in units of dB. The larger the PSNR value, higher is the quality of the resulting image. This is widely used parameter for quality assessment of degraded watermarked image.

RESULTS AND DISCUSSION

The degraded images as a result of various geometric attacks are shown in table 2. The sample images used are Tulip, Lena, Cameraman and Elaine. The results for cropping and row column blanking attack with varying levels of degradation are shown for Tulip image in table 3. The results are depicted for watermarked images with PSNR values around 40dB in the absence of any of these attacks. The sample results are shown for different images are shown. The quality of watermarked image is degraded significantly. This is observed by human vision as well as by PSNR values. Successful extraction of watermark from seriously degraded watermarked image indicates robust image watermarking.

Table 2 Results for Geometric Attacks




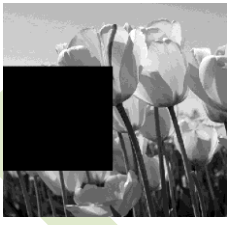


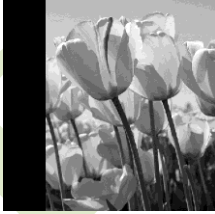


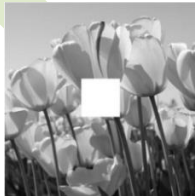
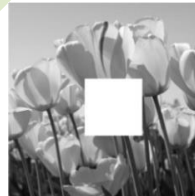


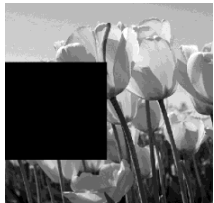
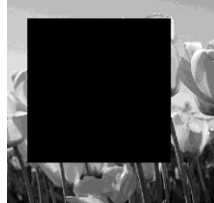

Geometric Attacks			
Cropping	Rotation	Flipping	Row-column Blanking
			
Scaling	Warping	Translation	Local Exchange of Pixels
			

Table 3 PSNR values for Different Geometric Attacks

Cropping Attack				
Cropping Ratio	10%	20%	30%	40%
Cropped Image				
PSNR (dB)	19.869	16.552	13.260	12.000
Row-Column Blanking Attack				
Rows and Columns blanked	R1-150, C1-150	R151-400, C1-250	R151-500, C151-500	R51-400, C51-400
Blanked Image				
PSNR (dB)	12.9211	10.0427	9.0217	7.2347

CONCLUSION

The analysis provides comprehensive study of possible geometric attacks on watermarked image with mathematical modeling. The results indicate substantial degradation of

watermarked image in the presence of geometric attacks. The validation is carried out visually as by quantitative metric. This provides guideline for robustness evaluation for extraction of watermark from watermarked image.

REFERENCES

- [1] Anil N. Bhure and Vaishali S Jabade, “*A Modified Approach of Image Steganography based on Block DCT and Huffman Encoding without Embedding Dictionary into Stego-Image*”, *Volume 94 - Number 8, May-2014*, pp. 24-27.
- [2] Biao-bing-huang and Shao-ziantang, “*A Contrast Sensitive Visible Watermarking Scheme*”, *IEEE feature article*, 2006, pp. 60-66.
- [3] Bo Chen, Hong Shen, “*A New Robust-Fragile Double Image Watermarking Algorithm*”, *Third International Conference on Multimedia and Ubiquitous Engineering*, 2009, pp. 153-157.
- [4] Der-Chyuan Lou , Hao-Kuan Tso, Jiang-Lung Liu “*A Copyright Protection Scheme For Digital Images Using Visual Cryptography Technique*”, *Computer Standards and Interfaces* 29, 2007, pp. 125-131.
- [5] Der-Chyuanlou, Hao-kuan Tso, Jiang-lungliu, “*A Copyright Protection Scheme for Digital Images Using Visual Cryptography Technique*”, *Computer Standards and Interfaces*, 2006, pp. 125-131.
- [6] Dr. M.A. Dorairangaswamy, B. Padmavathi, “*An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images*”, *IEEE, TENCON*, 2009, pp. 1-6.
- [7] Jun Sang and Mohammad S. Alam, “*Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/Semi fragile Digital Image Watermarking*,” *IEEE Transactions on Instrumentation And Measurement*, Vol. 57, No. 3, March 2008, pp.595-606.
- [8] M.F. Fahmy and G. Fahmy, “*A Quasi Blind Watermark Extraction of watermarked Natural Preserve Transform Images*”, *IEEE Ineternational Conference on Image Processing*, 2009, pp.3665-3668.
- [9] Mr. Manjunatha Prasad. R, Dr.Shivaprakash Koliwad “*A Comprehensive Survey of Contemporary Researches in Watermarking for Copyright Protection of Digital Images*”, *International Journal of Computer Science and Network Security (IJCSNS)*, Vol.9, No.4, April 2009, pp. 91-102.
- [10] Mohammad Abdullatif, Akram M. Zeki, Jalel Chebil, Teddy Surya Gunawan “*Properties of digital image watermarking*”, *IEEE 9th International Colloquium on Signal Processing and its Applications (CSPA)*, March-2013, pp. 235-240

- [11] Santa Agreste, Guido Andaloro, Daniela Prestipino, Luigia Puccio, “*An Image Adaptive Wavelet Based Watermarking of Digital Images*”, *Science Direct Journal of Computational and Applied Mathematics*, 2006, pp. 1-9.
- [12] Thi Hoang Ngan Le, Kim Hung Nguyen, Hoai Bac Le, “*Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking Tools*”, *Second IEEE International Conferences on Advances in Multimedia*, 2010, pp.67-73.
- [13] Vaishali S. Jabade and Sachin R. Gengaje, “*Comprehensive Survey of Image Watermarking*”, *International Journal of Advances in Engineering and Technology (IJAET)*, Volume 6, Issue 3, July 2013, pp. 1271-1282.
- [14] Vaishali S. Jabade and Sachin R. Gengaje, “*Bi-orthogonal Wavelet based Adaptive Image Watermarking using Human Visual System and Fuzzy Inference System*”, *International Journal of Computer Applications (IJCA)*, (0975 – 8887) Volume 72– No.14, May 2013, pp. 39-43.
- [15] Vaishali S. Jabade and Sachin R. Gengaje, “*Logo based Image Copyright Protection using Discrete Wavelet Transform and Fuzzy Inference System*”, *International Journal of Computer Applications (IJCA)*, (0975 – 8887) Volume 58– No.10, November 2012, pp. 22-28.
- [16] Vaishali S. Jabade and Sachin R. Gengaje, “*Literature Review of Wavelet Based Digital Image Watermarking Techniques*”, *International Journal of Computer Applications (IJCA)*, (0975 – 8887) Volume 31– No.1, October 2011, pp. 28-35.
- [17] Vaishali S. Jabade and Sachin R. Gengaje, “*Performance Evaluation of DWT and FIS Based Digital Image Watermarking*”, *International Journal of Computer Applications (IJCA)*, (0975 – 8887) Volume 4, Issue 1, January 2016, pp. 892-900.
- [18] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, “*A Survey of Digital Image Watermarking Techniques*”, *3rd IEEE International Conference on Industrial Informatics (INDIN)*, 2005, pp.709-713.
- [19] Wan Adnan, W.A.; Hitam, S.; Abdul-Karim, S., Tamjis, M.R., “*A review of image watermarking*”, *Research and Development, SCORED*, 2003, pp. 381-384.
- [20] Wen-Nung Lie, Guo-Shiang Lin, Sheng-Lung Cheng, “*Dual Protection of JPEG Image Based on Informed Embedding And Two Stage Watermark Extraction Techniques*”, *IEEE Transactions on information forensics and security*, Vol. I, 2006, pp. 330-341.