Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 93 (2016) 808 – 815
Procedia Computer Science

6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

An Invisible Logo Watermarking using Arnold Transform

Saikrishna N[1,*], Resmipriya M G[1]

[a]*PG Scholar,Dept. of Computer Science & Engineering,Amal Jyothi College of Engineering Kanjirapally, Kottayam,686518*
[b]*Assistant Professor,Dept. of Computer Science & Engineering,Amal Jyothi College of Engineering Kanjirapally, Kottayam,686518*

Abstract

Digital watermarking is the process of hiding information into the digital content. The method of embedding a smaller logo image into the host image is called logo watermarking. The system proposes an invisible and secure watermarking. The key entered initially determine the location of embedding and thus classified the host image to white and black textured regions. The logo image is then transformed using Arnold transform. Discrete Wavelet Transform (DWT) technique is employed for embedding the transformed logo into the white textured regions. Watermark extraction is done by entering the same key which was already entered during embedding. The system is secure and the logo is imperceptible within the host image. Finally for analysis, PSNR value has been used as a metric for determining the quality of the recovered image.

Peer-review under responsibility of the Organizing Committee of ICACC 2016
Keywords: Arnold Transformation; Histogram Oriented Gradients(Hog); Discrete Wavelet Transform (DWT)

1. Introduction

The method of permanently hiding or embedding an image over the host image is called digital image watermarking. The watermark then be extracted for copyright ownership identification[1]. Invisible watermarking is the method in which data embedded is invisible or undetectable to human eyes. Invisible watermarking notifies the illegal use of images to its exact owner or the legal user. Thus these methods are useful as a means of identifying the ownership. Digital tampering of photos which is shared over several social networking websites is becoming a major issue now a days. That is the original image may undergo various forms of geometric and non-geometric attacks like rotation, scaling, translation and compression, motion blur, Gaussian noise respectively. Robustness is the property to resist against these types of both geometric and non-geometric attacks. Invisible watermarking is useful mainly in those applications like embedding QR (Quick Response)[13] codes in images that is watermarks may not be visible with the naked eyes. Other applications include image quality assessment, medical imagery, multimedia transmission etc. Watermark in the form of image,audio or even text cannot be recognized from the host image but it can be perceptible after the extraction procedure. This important property of watermark is called invisibility. Security ensures that water-

[*] Corresponding author
E-mail address: nsaikrishna92@gmail.com

Peer-review under responsibility of the Organizing Committee of ICACC 2016
doi:10.1016/j.procs.2016.07.299

mark is accessible only to authorized parties. Thus the main properties of watermarking are imperceptibility, security robustness.

The major challenge of logo watermarking is to handle variety of attacks, both geometric and non-geometric. Another challenge is to make the logo invisible within the host image. The entire host image should be utilized instead of a part. After the extraction procedure, the watermark need to be original or in an understandable form for effective comparison. The algorithm must be robust enough to survive various attacks, imperceptible, secured for an effective watermarking. The system must be well enough to handle many logos. The two main domains of watermarking are spatial domain and transform domain[14]. Spatial domain includes the direct modification of the pixel values. These methods are inexpensive but not robust enough to survive different attacks. Transform domain techniques transforms the pixels and the transformation can be based on Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). These techniques are more robust and imperceptible than the spatial domain. DCT employs block based processing but coefficients are not decorrelated. Thus for an efficient system, watermarking based on wavelet transform obtains better result.

The proposed system aims at introducing an invisible and secured grey scale logo watermarking. Major steps of the system include transformation, embedding and extraction. Initially the user need to enter the key and then using the rand function, uniformly distributed locations are determined from the provided order. The system then segments the host image into white textured and black textured regions. Next step is to transform the logo image using Arnold transformation and rotation. The locations of white textured region is used for embedding. Discrete Wavelet Transform is employed for both embedding and extraction. Analysis is done on the quality of both watermarked and recovered image using the PSNR (Peak Noise-to-Signal Ratio).

Section 2 is a study of existing literature. It gives a brief introduction into the basics of digital watermarking, a description of some existing techniques and previously known methods and procedures on watermarking. Section 3 gives the detailed overview of the implementation, and the description of main modules. Section 4 goes on to summarize the results of the experiment in terms of the quality of embedded and the recovered image. Finally the last section concludes the paper and gives a future scope to the implemented system.

2. Related Work

Digital watermarking is used for authentication, integrity, or to show the identity of its owners. Steganography and watermarking employ hiding techniques to embed the data. Steganography aims for imperceptibility to human senses where as digital watermarking tries to control the robustness as the top priority. Watermarking is the technique of direct embedding of information into the host or the original content. Watermarking algorithms has been proposed for image, audio, video, document and graphics. According to the type of working, watermarking techniques are being classified into spatial and transform domain. In spatial domain, watermark embedding is applied directly to the pixel values. The images are manipulated by changing one or more of the bits that make up the pixels of the image. Least Significant Bit (LSB) and M Sequences are the examples of spatial domain. Where as in transform domain, there occurs a transformation of image into a set of components. Examples include Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). DWT techniques transform the entire image as compared to DCT. Coefficients are correlated in DCT and causes blocking artefacts. Thus considering the manipulation side, DWT performs the fast and robust form of watermarking technique. Transform domain watermarking is useful in taking advantage of perceptuality in the embedding process, for designing watermarking techniques, and for direct embedding of compressed bit streams. Frequency domain watermarking techniques are used to acquire the general properties of watermarking such as security, imperceptibility and robustness.

Visible watermarks are detectable by human eyes and are very easy to remove. In invisible watermarking, data embedded is invisible, that is watermark is imperceptible when placed within the host image. The watermark needs to be imperceptible so that the view of the image is unaffected. Invisible watermarking is found to be better than visible watermarking as it is visually imperceptible after embedding and visually recognizable when extracted. Block based scheme deals each blocks individually and can survive both geometric and non-geometric attacks and hence ensures complete robustness. Thus most of the watermarking scheme focus on block oriented technique and consider each block as a separate image and perform corresponding manipulations.

Other than DCT or DWT based techniques another method of watermarking called SVD[3] (Single Value Decomposition) has been introduced. In two-dimensional DWT, each level of decomposition produces four bands of data denoted by LL, HL, LH, and HH. The LL sub band can further be decomposed to obtain another level of decomposition. After the decomposition, single value decomposition procedure is applied to each band, and modify the singular values of the cover image with the singular values of the visual watermark. SVD based techniques may modify only the singular values and leave the orthogonal matrices. These methods do not embed the watermark completely into the host image. When the scaling factor is reached to an unreasonable value, the image becomes brighter and hence results in low visual quality. Thus SVM based methods are less effective as compared to DWT methods.

Copyright protection is attained by an effective technique called Human Visual System(HVS)[4] models,which is applied into watermarking scheme. A number of factors affect the noise sensitivity of the human eye like frequency band, luminance, texture and proximity to an edge. Human eye is less sensitive to the areas of the image where brightness is high and in high frequency sub bands. Sensitivity of human eye to noise in textured area is less and it is more near the edges. The system is using a masking function for calculating the weight factors for wavelet coefficients of the host image. The method of embedding completely depends on the weights. HVS is an important characteristic need to be considered in watermarking.

The watermarking scheme employs a technique called Arnold transform[6] for texturizing the logo. This scheme enhances the security of watermarking. The texturization procedure is done to enhance the similarity with the host image. There are composite watermarking algorithm[10] which performs embedding based on modulus and additive based insertion. The logo has been pseudo randomly shuffled and scaled and embedded in the LL sub band of the image using modulus based addition. Logo is transformed based on DCT and is embedded into the perceptually significant blocks of the LH, HL, and HH sub bands using weighted addition of coefficients. These weights are determined based on visual masking.

3. Proposed Methodology

The system introduces an invisible logo watermarking based on texturization. A host image of size 512×512 and a small logo image of size 64×64 is taken. The host image is segmented into 64 blocks where each block is of size 64×64. Initially, a key should be entered before the embedding procedure. This key determines the locations for embedding. Embedding and extraction procedure is done based on Discrete Wavelet Transform (DWT). The main stages of the system is explained below:

3.1. Texture Segmentation Based on Key

Host image and the logo image are loaded. The next procedure is to separate the textured and non-textured regions of host image. A key need to be entered before the embedding procedure. Rand function uses a parameter called seed which provides a random controlling and specific ordering. Randperm function uses maximum location as the parameter and generates uniformly distributed locations having a defined order. Then a binary image showing black and white textured regions is being generated. All the even locations are textured as white and the other one as black. That is, every locations used for embedding constitutes the white textured region, where we may perform embedding. After getting the locations of embedding, the basic embedding procedure is done. This procedure is also repeated in the extraction procedure. That is, before extraction the user needs to enter the same key which was already entered during embedding. After specifying only the same key during extraction, the exact embedded image can be recovered. This phase mainly provides security in watermarking.

3.2. Logo Scrambling via Arnold Transform

After the segmentation procedure into white and black textured regions, next step is to apply some transformation to the logo using Arnold transform. This is to enhance security to the logo image. That means, the logo image is not embedded as such, instead a transformed logo is used for embedding. On the extraction phase, inverse Arnold transform is applied.

3.2.1. Arnold Transform

Arnold transform is a two-dimensional mapping which transforms each coordinate (x,y) in the logo image to a new coordinate (x$^{'}$, y$^{'}$) and is given by the following equations,

$$x' = a_1 x + a_2 y + modL \tag{1}$$

$$y' = a_3 x + a_4 y + modL \tag{2}$$

where the parameters may satisfy, $a_1 * a_4 - a_2 * a_3$=∓1 and the parameter L×L is the size of the logo image. An adaptive logo-scrambling performs an iterative procedure which results in the generation of scrambled images. Arnold transformation is a periodic and invertible mapping. Besides, the Arnold transformation is valid for square images only. The Arnold transformation is used to scramble the digital images and has many applications, especially in digital watermarking.

Rotation for the logo is applied for angles 90,180 and 270. Here the number of iteration is 4. The ability to scramble and descramble may enhance the security in watermarking. The figure 3.2.1 shows the logo image and the resultant Arnold Transform applied on the same is shown in figure 3.2.1.

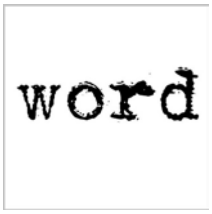

Fig. 1. Logo image of size 64×64

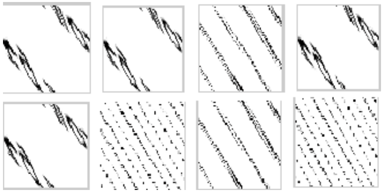

Fig. 2. Results of Arnold Transform applied on logo image of size 64×64

3.2.2. Histogram Of Oriented Gradients

Histogram Of Oriented Gradients(HOG) is a feature descriptor used in different areas of image processing. Initially HOGs of watermarked and the host image is computed. This helps in finding out the differences or the dissimilarities among the two images. We need to minimize the dissimilarity and hence to strengthen the watermark embedding. HOG is an important factor to point out the major dissimilarities. Arnold transformation is applied to reduce those dissimilarities that is to make the images visibly similar.

3.3. Watermark Embedding in DWT domain

There are mainly two inputs for embedding. They are host blocks from the first stage and scrambled logos from the next stage. After finding out the minimum dissimilarity estimate a best location has been identified to embed the scrambled logo image. Using the two level DWT(Discrete Wavelet Transform) based embedding scheme, embed the scrambled logo image into corresponding block of host image. Human Visual System (HVS) method is employed here. The method explains that our eyes are more attracted to the areas having less frequencies and more adjusted to the high frequency areas. Thus the LL subband has least chance to embed the hidden information. Where as the other bands like LH,HL,HH has got the chances to embed more data. Watermark embedding can be explained based on the following equation.

$$LL1 = \alpha * ll + LL; \tag{3}$$

$$LH1 = \alpha * lh + LH; \tag{4}$$

$$HL1 = \alpha * hl + HL; \tag{5}$$

$$HH1 = \alpha * hh + HH; \tag{6}$$

Here α is the weight factor for embedding. HH, LH, HL and HH are the subbands of host image. ll, lh, hl and hh are the subbands of transformed logo image. The subbands LL1, LH1, HL1 and HH1 are finally constitute the embedded image or the watermarked image.

3.4. Watermark Extraction

The watermark extraction procedure is also done based on DWT. After the subtraction of all subbands of host image from the subbands of watermarked image, the scrambled logo or the watermark is obtained. In order to extract the scrambled or the texturized logo inverse DWT is used. The number of iterations in Arnold transformation is used to average transformed logos. Finally we will get the exact logo image from the watermarked image.

4. Experimental Results

Watermark embedding and extraction is applied with respect to mainly 4 host images. The watermarked images appears to be similar to the original host image. This proves that the system supports invisibility. That is the watermark or the logo image is completely hidden within the host image and is not visible to our eyes. The figure4 showing various host images along with the watermarked images. Initially a key need to be entered before embedding. In the extraction phase the same key which was entered before must be entered. If the keys are different we wont be able to recover the exact logo image. This proves that the system is more secure.

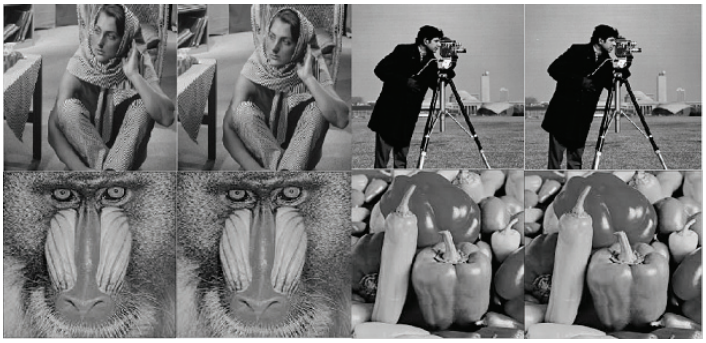

Fig. 3. Host Images and Watermarked Images

PSNR is used as the metric for comparing original logo image and the restored image. The general equation for measuring the PSNR value is shown below and here MSE is the Mean Square Error.

$$PSNR = 10 * log10((255 * 10)^2/MSE \tag{7}$$

The restored image shows better result of PSNR if there is no noise. This is tested for various host images and is shown in the table 4. Thus the proposed system shows an average PSNR value of 48 in the absence of noise. Higher the value of PSNR indicates effective watermark embedding or the restored image and the watermarked image is of good quality. The table4 shows that the system works well with the specified host images and the result of PSNR measurement is almost similar for all host images.

Salt and Pepper noise is used for analysis purpose. This is a form of noise mostly seen on images. It presents itself as sparsely occurring white and black pixels. Initially the noise levels are entered manually. After that the PSNR value of the same is calculated using the above mentioned equation and the corresponding graph is plotted. The graph, PSNR vs. Noise Level is shown below.

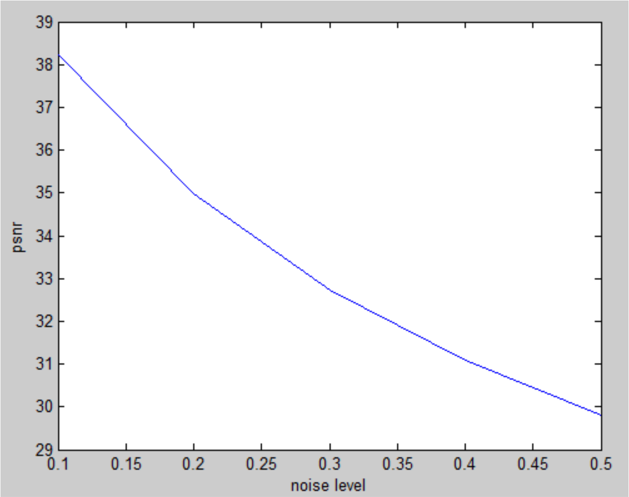

Fig. 4. PSNR vs. Noise level

5. Conclusion and Future Works

This paper presented an algorithm for grey scale logo watermarking. Initially a key is used to decide the positions of embedding so that the logo image can be extracted by entering the same key. The main idea of this approach is to transform the logo image using arnold transformation. Embedding is done based on Discrete Wavelet Transform and Human Visual System. The proposed system works successfully by proving invisibility and security and estimated the PSNR value.

Future enhancements can be applied on ensuring more robustness against various geometric and non-geometric attacks. Also by using various sets of logos and host images the system yields better performance than any other competing methods. The system can also be applied to color images.

References

1. C. I. Podilchuk and E. J. Delp, Digital watermarking: algorithms and applications, IEEE Signal Proc Mag, vol. 18, no. 3, pp. 3346, 2001.
2. X. Zhao and A. T. S. Ho, An introduction to robust transform based image watermarking techniques, Springer, Intelligent Multimedia Analysis for Security Applications, vol. 282, pp. 337364, 2010.
3. E. Ganic and A. M. Eskicioglu, Robust embedding of visual watermarks using dwt-svd, J. Electronic Imaging, vol. 14, no. 4, 2005.
4. A. A. Reddy and B. Chatterji, A new wavelet based logo-watermarking scheme, Pattern Recogn, vol. 26, pp. 10191027, 2005.
5. H. Bay, A. Ess, T. Tuytelaars, and L. V. Gool, Speeded-up robust features (surf), Computer Vis. Image Und., vol. 110, pp. 346359, 2008.
6. Mehran Andalibi and Damon M. Chandler, ”Digital Image Watermarking via Adaptive Logo Texturization” IEEE Transactions on Image Processing,pp 1-14,2015
7. V. P. Reddy and D. S. Varadarajan, An effective wavelet-based watermarking scheme using human visual system for protecting copyrights of digital images, International Journal of Computer and Electrical Engineering, vol. 2, pp. 17938163, 2010
8. C. C. Lai and C. C. Tsai, Digital image watermarking using discrete wavelet transform and singular value decomposition, IEEE Transactions on instrumentation and measurement, vol. 59, no. 11, 2010.

9. C. Jin, F. Tao, and Y. Fu, Image watermarking based hvs characteristic of wavelet transform, in International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2006
10. E. First and X. Qi, A composite approach for blind grayscale logo watermarking, in IEEE Int. Conf. Image Proc, Vol 3, pp. 265-268, 2007.
11. M. A. Fischler and R. Bolles, Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography, Comm. of ACM, vol. 24, no. 6, pp. 381395, 1981.
12. M. Natarajan and G. Makhdumi1, Safeguarding the digital contents: Digital watermarking, DESIDOC Journal of Library and Information Technology, vol. 29, no. 2, pp. 2935, 2009.
13. S. Vongpradhip and S. Rungraungsilp, Qr code using invisible watermarking in frequency domain, in ICT and Knowledge Engineering, pp. 47 - 52, 2012.
14. R. Halder, S. Pal, and A. Cortesi, Watermarking techniques for relational databases: survey, classification and comparison, Journal of universal computer science, vol. 16, no. 21, 2010.
15. N. Dalal and B. Triggs, Histograms of oriented gradients for human detection, in IEEE Computer Society Conf. Comp. Vis. and Pattern Recogn., vol. 1, pp. 886893, vol. 1, June 2005, pp. 886893 vol. 1.
16. Ravi Kumar, Garima Garg, ”A Review OnGUI Implementation of Efficient Robust Digital Watermarking using 3-Discrete wavelet Technique” IJCT,vol.2,issue.3, June 2015

Table 1. PSNR values without noise

Metric	Barbara	Mandril	Cameraman	Peppers
PSNR (dB)	48.92	48.89	48.90	48.89