2020

A MONOGRAPH ON WATERMARKING OF IMAGE USING ROBUST HISTOGRAM SHAPE METHOD

Mrs. Swati Nitanaware

Apoorva B. Sharma

6/7/2020

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

A MONOGRAPH ON WATERMARKING OF IMAGE USING ROBUST HISTOGRAM SHAPE METHOD

Mrs. Swati Nitanaware

Apoorva B. Sharma

Publishing Partner:
IJSRP Inc.
www.ijsrp.org

ISSN 2250-3153
9 772250 315302

Preface

With the fast growth of communication networks and advances in multimedia processing technologies, multimedia protection has become a serious problem and rapid development of modern communication networks, information is transmitted with speeds never seen before. At the same time, illegally manipulated copies of digital media can be easily transmitted and distributed. As a result, copyright protection has become a major issue worldwide. Digital watermarking is a promising technique to tackle this problem. While digital watermarking can be applied to audio, image and video we focuses on image watermarking. A good image-watermarking method should be imperceptible, robust, and secure. Imperceptibility means that watermarks should be perceptually unobtrusive. Robustness indicates the ability of correctly extracting watermarks after undergoing different kinds of attacks. There are two types of attacks, which are signal processing attacks (e.g., compression, filtering, and noise addition) and geometric attacks (e.g., scaling, rotation, shearing, cropping, and random bending). Security refers to the resistance to unauthorized watermark decoding without knowing the secret key. Over the last decade, various image- watermarking methods have been developed. Many of these methods are robust to common signal processing attacks but do not cope well with geometric attacks. For example, some methods are resistant to median filtering and JPEG compression but very sensitive to rotation. To tackle geometric attacks, various techniques have been utilized in image watermarking.

Those techniques can be broadly classified into nonblind and blind watermarking techniques,

respectively. The nonblind watermarking techniques need to use the host image for watermark extraction at the decoding end. Thus, their practical usage is very limited. On the other hand, the blind watermarking techniques do not require the information of the host image in the decoder, which makes them more suitable for real-world applications. One of the blind method is

exhaustive search which is carried out at the decoding end to search the embedded watermarks from the received image. The exhaustive search-based methods are very expensive in computation. Moreover, their false detection probability is high. Median filtering and JPEG compressions were overcame by Multiscale Gradient Direction Quantization method.

Publication Partner:
International Journal of Scientific and Research Publications (ISSN: 2250-3153)

Copyright and Trademarks

Authors

Ms. Swati R. Nitnaware
Asst. Prof. Department of Electronics and Telecommunication
Yeshwantrao Chavan College of Engineering,
Nagpur

Apoorva B. Sharma
M-Tech Department of Electronics Engineering
Yeshwantrao Chavan College of Engineering,
Nagpur

Table of Content

LIST OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

DCT	Discrete cosine transform
DWT	Discrete wavelet transform
DFT	Discrete fourier transform
JPEG	Joint photographic expert group
RBA	Random Bending Attack
PSNR	Peak signal to noise ratio
SSIM	Structural similarity index measure
BER	Bit error rate

ABSTRACT

On an image when geometric attacks or signal processing are introduced during decoding process then the watermark embedded image should be extracted correctly. Among both the attacks which are geometric attacks and signal processing attacks the geometric attacks are difficult to cope in image watermarking. A new methodology is proposed to deal with both the attacks, as well as other common attacks. Initially in the embedding process, the host gray scale image is first preprocessed by a Gaussian low-pass filter. The histogram of the filtered image is constructed. Mean of the histogram is calculated. According to this mean, gray scale pixel values which are less than mean are chosen for watermark embedding. Pixel group selection is done. A scheme is proposed to insert watermarks into the chosen pixel groups.. At the decoding end, the watermarked pixel groups are identified and inserted watermarks are extracted from them for both cases that is without attacks and with attacks.The respective results of embedding process, decoding process and certain attacks are obtained in MATLAB R2016a.

INTRODUCTION

1.1 Overview

Digital watermarking is one of the promising methods to communicate secret data in an image, video or audio, visibly or invisibly to protect the owner‟s copyrights. Copyright protection of digital contents is the need of time as it has become very important to protect the data from any malicious user while existing in the digital world. Digital watermarking is the better solution for copyright protection than encryption and steganography. Digital watermarking is efficient enough to identify the original copyright owner of the contents - an image, a plain text, an audio, a video or a combination of all.

While digital watermarking can be applied to image, audio and video this proposed methodology focuses on image watermarking. A good image-watermarking method should be imperceptible, robust, and secure. Imperceptibility means that watermarks should be perceptually unobtrusive. Robustness means the ability of correct extraction of watermarks after undergoing different kinds of attacks. There are two types of attacks; signal processing attacks (e.g. filtering, compression and noise addition) and geometric attacks (e.g., cropping, scaling, rotation, shearing, and random bending). Security refers to the resistance to unauthorized watermark decoding without knowing the secret key.

Any watermarking scheme consists of three parts: the watermark, the encoding process and the decoding process. The watermarking algorithm incorporates the watermark into the original image in the encoding process and extracts the same watermark in the decoding process. Decoding is done with and without attacks.

1.2 Literature Survey

Tianrui Zong, Young Xiang, Wanlei Zhou and Gleb Beliakov," Robust Histogram Shape-Based Method for Image Watermarking" described an overview of the work done on removing cropping and random bending attacks in image watermarking. In this paper they proposed a novel image-watermarking method to deal with these attacks, as well as other common attacks. In the embedding process, they first preprocessed the host image by a Gaussian low-pass filter followed by histogram construction and pixel group selection. Watermark image is inserted into a selectd pixel groups. For security purpose they used a secret key. At the decoding end, based on the available secret key, the watermarked pixel groups are identified and watermarks are extracted from them.

L. Wang, H. Ling, F. Zou, and Z. Lu, "Real-time compressed domain video watermarking resistance to geometric distortions," describes a proposed geometrically invariant watermarking method by exploiting the fact that the histogram shape of the low frequency subband in DWT domain is insensitive to various geometric distortions. Second, they used a fast intertransformation to obtain the DWT coefficients directly from the compressed data instead of using the traditional method that first decompresses the block DCTs of frames into pixel data and then applies DWT to these data. Thus, they significantly reduce the computational cost and meet the real-time requirement. This algorithm can be used for data hiding in many applications such as authentication and copyright protection.

H. Zhang et al., "Affine Legendre moment invariants for image watermarking robust to geometric distortions," proposed a watermarking scheme robust to a wide range of attacks: geometric distortion, filtering, compression, and additive noise. The major contribution of this paper relies on two aspects. The first one is the derivation of a set of affine invariants based on Legendre moments. Those invariants can be used for estimating the affine transform coefficients applied to one image. The second one is the use of these affine Legendre moment invariants for watermark embedding, detection and extraction. The proposed method is more robust than others based on geometric moments. The limitation of the proposed algorithm is that it is not robust to

image cropping and histogram equalization, a common problem for the moment-based watermark algorithms.

J.-S. Tsai, W.-B. Huang, and Y.-H. Kuo, "On the selection of optimal feature region set for robust digital image watermarking," describes a novel feature region selection method for robust digital image watermarking is proposed. A novel method based on the simulated attacking approach and the GA (geometric attack) based MDKP (multidimensional knapsack problem) solving procedure is developed to select the most adequate feature regions for robust digital image watermarking under the constraint of preserving image quality. Compared with other feature-based watermarking methods, the robustness against various attacks is significantly improved by the proposed method, and the image quality after watermarking is still preserved. The proposed method consumes too much computation time in measuring the robustness of feature regions due to the simulated attacking.

N. K. Kalantari, S. M. Ahadi, and M. Vafadust, "A robust image watermarking in the ridgelet domain using universally optimum decoder," proposed a robust image watermarking scheme in the ridgelet transform domain. The watermark data is embedded in selected blocks of the host image by modifying the amplitude of the ridgelet coefficients which represent the most energetic direction. Since the probability distribution function of the ridgelet coefficients is not known, they propose a universally optimum decoder to perform the watermark extraction in a distribution independent fashion. Decoder extracts the watermark data using the variance of the ridgelet coefficients of the most energetic direction in each block. Furthermore, since the decoder needs the noise variance to perform decoding, a robust noise estimation scheme is proposed. Moreover, the implementation of error correction codes on the proposed method is investigated. The proposed method shows outstanding robustness against common attacks, especially additive white noise and JPEG compression.

L. Xin-Wei, G. Bao-Long, L. Lei-Da, and S. Hong-Xin, "A new histogram based image watermarking scheme resisting geometric attacks," proposed a new histogram modification scheme considering the visual quality of the watermarked image. They use the mean pixel value of divided blocks to calculate histogram and the mean square error to select blocks to be modified based on HVS. They obtained a good trade-off

between robustness to geometric attacks and common image processing attacks by adjusting the block size. This is complete embedding scheme and the reverse of this is done in decoding scheme. The proposed approach has an excellent robustness against geometric attacks and some normal attacks, such as adding noise and JPEG compression. In the proposed scheme, they have presented two optimization methods based on Xiang et al.‟s method from histogram modification and pixel modification respectively.

S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," presented an image watermarking scheme by the use of two statistical features (the histogram shape and the mean) in the Gaussian filtered low-frequency component of images. A key-based PN sequence is successfully inserted by modifying the histogram shape, which is computed from the low-frequency component of Gaussian filtered images by referring to the mean. The watermark can be detected without knowledge of original images by sharing the exploited private key in the detector. However, the histogram-based watermarking have its limitation for histogram equalization since this operation will distort the histogram shape much.

J. F. Lichtenauer, I. Setyawan, T. Kalker, and R. L. Lagendijk,"Exhaustive geometrical search and the false positive watermark probability," describes that image and key dependency in the watermark detector leads to different false positive detection probabilities for geometrical searches for different images and keys. Furthermore, the image and key dependency of the tested watermark detector increases the random-image-random-key false positive detection probability. False positive detection probability, in the correlation-based watermarking scheme they used in this research, is dependent on image content and detection keys. Because of these dependencies, varying over transforms only, while keeping the other factors constant, like in a normal geometrical search, gives a different false positive detection probability in a geometrical search for each choice of the constant factors on which the watermarking scheme is dependent.

P. Dong, J. G. Brankov, N. Galatsanos, and Y. Yang, "Geometric robust watermarking based on a new mesh model correction approach," describes a

watermarking scheme based on a new deformable mesh model to combat geometric attacks. In this paper they proposed a new objective function to estimate the DF. This objective function consists of two terms. The first term captures the matching error between the original and the attacked watermarked image, and the second term captures the regularity of the DF. This new objective function forces the smoothness of the DF, instead of mesh regularity, so that it can capture effectively the distortion in the attacked image. The estimated DF is then used for distortion compensation. They applied a CDMA based multi-bit watermarking scheme for the embedder , by virtue of its property of high- robustness to common signal processing operations.

N. K. Kalantari, S. M. Ahadi, and M. Vafadust, "A robust image watermarking in the ridgelet domain using universally optimum decoder," describes a non – blind method to reverse the effect of local geometric distortions, in order to recover the signature from image close to the original one . Another non – blind method with the same objective is introduced, making use of representative feature points at multiple resolutions. They presented in this paper a compensation technique allowing to retrieve a watermark in an image the original image, or its edges. For this they use 2D mesh, in order to compensate parts of geometric distortion that could be introduced by softwares such as Stirmark. In order to illustrate the usefulness of the compensation on attacked images, they used two watermarking techniques : classical spread spectrum algorithm proposed by Cox etal. (the watermark is embedded into a selected set of DCT coefficients) and a wavelet based watermarking technique.They have shown that it allows to retrieve the watermark from an attacked image, if this is watermarked in its DCT (spread spectrum technique) or its DWT (significant wavelet coefficients quantization) representation.

N. F. Johnson, Z. Duric and S. Jajodia, "Recovery of watermarks from distorted images," describes a method for the recovery of original size and appearance of images based on the concept of identification marks (fingerprints"); the method does not require the use of the "original" image, but only a small number of salient image points. However, embedded watermarks may fail to be recognized due to accidental corruption or attack by cropping and/or affine distortions (e.g., rotation, scaling, and blurring) . This hampers the ability to locate and identify watermarked images over distributed networks such as the Internet. Using this method, it is possible to recover

original appearances of distorted images. The restored image can be used to recover embedded watermarks.

S. Pereira, J. J. K. O. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun,"Template based recovery of Fourier-based watermarks using log - Polar and log- log maps," describes a method for the secure and robust copyright protection of digital images. The authors presented an approach for embedding a digital watermark into an image using the Fast Fourier transform. To this watermark is added a template in the Fourier transform domain to render the method robust against rotations and scaling, or aspect ratio changes. The watermark is composed of two parts, a template and a spread spectrum signal containing the information or payload. The template contains no information in itself, but is used to detect transformations undergone by the image. Once detected, these transformations are inverted and then the spread spectrum signal is decoded. The spread spectrum signal contains information such as the owner of the image, a serial number and perhaps flags which indicate the type of content e.g. religion, pornography, or politics. This can be useful for indexing images or even for tracking pornography on the web.

1.3 Problem Statement Description

A common need has been observed for making the Digital Watermarking process a real-time application. From the various papers referred, it has been observed that there are various methods that are available for building a watermarking technique. A lot of work has been carried to tackle with both geometric and signal processing attacks but there were problems like less robustness and less security.

So, there was a need to build a highly robust and highly secured watermarking technique which is capable to resist both geometric and signal processing attacks. Also, the watermarking technique should be invisible to make it secure. So, this objective was also taken into consideration while building the watermarking technique.

1.4 Objectives

The thesis objectives are as follows:-

- To design a watermarking technique.
- To design a watermark embedding process .
- To design a watermark decoding process .
- To evaluate the robustness of the watermark decoding algorithm against several attacks.

1.5 Overview

The thesis describes the designing and implementation of watermarking algorithm applicable on grayscale images and will also describe the embedding and decoding process.

Chapter 2 contains the literature review of the papers related to the work.
Chapter 3 contains the work done related to embedding and extraction process of watermarking Algorithm.

Chapter 4 describes the result and conclusion of the embedding and extraction process of watermarking algorithm in MATLAB R2016a.

Chapter 5 gives the Summary, Conclusion of the work carried and implemented and also the future work that can be done related to the work.

REVIEW OF LITERATURE

2.1 Tianrui Zong, Young Xiang, Wanlei Zhou and Gleb Beliakov," Robust Histogram Shape-Based Method for Image Watermarking" IEEE Transactions on circuits and system for video technology,vol.25,No.5,717-729, 2015 .

This paper provided an overview of the work done on removing cropping and random bending attacks in image watermarking. In this paper they proposed a novel image-watermarking method to deal with these attacks, as well as other common attacks.

In the embedding process, they first preprocessed the host image by a Gaussian low-pass filter. For security purpose they used a secret key. Secret key is used to randomly select a number of gray levels . Then a histogram of the filtered image with respect to these selected gray levels is constructed. After that, a histogram-shape-related index is introduced to choose the pixel groups with the highest number of pixels and a safe band is built between the chosen and nonchosen pixel groups. A watermark-embedding scheme is proposed to insert watermarks into the chosen pixel groups. The usage of the histogram-shape-related index and safe band results in good robustness. Moreover, a novel high-frequency component modification mechanism is also utilized in the embedding scheme to further improve robustness.

At the decoding end, based on the available secret key, the watermarked pixel groups are identified and watermarks are extracted from them. A safe band which is introduced between the selected pixel groups and the nonselected pixel groups to improve robustness to geometric attacks. Furthermore, a novel HFCM scheme is proposed to compensate the side effect of Gaussian filtering, which further enhances robustness. Due to the usage of secret key, the proposed watermarking method is also secure.

2.2 L. Wang, H. Ling, F. Zou, and Z. Lu, "Real-time compressed domain video watermarking resistance to geometric distortions," IEEE MultiMedia, vol. 19, no. 1, pp. 70–79, Jan. 2012.

The paper describes a proposed geometrically invariant watermarking method by exploiting the fact that the histogram shape of the low frequency subband in DWT domain is insensitive to various geometric distortions. Second, they used a fast intertransformation to obtain the DWT coefficients directly from the compressed data instead of using the traditional method that first decompresses the block DCTs of frames into pixel data and then applies DWT to these data. Thus, they significantly reduce the computational cost and meet the real-time requirement.

In this work, they presented a real-time video watermarking scheme with high robustness in the compressed domain. Although they only tested the proposed scheme on video in the MPEG-1 and MPEG-2 format, it is suitable for other DCT-based compressed videos such as MPEG-4 and H.264 because the DWT domain could be directly acquired from block DCTs of any size. This algorithm can be used for data hiding in many applications such as authentication and copyright protection.

2.3 H. Zhang et al., "Affine Legendre moment invariants for image watermarking robust to geometric distortions," IEEE Trans. Image Process.,vol. 20, no. 8, pp. 2189–2199, Aug. 2011.

In this paper, they proposed a new watermarking approach which allows watermark detection and extraction under affine transformation attacks. The novelty of their approach stands on a set of affine invariants which are derived from Legendre moments. Watermark embedding and detection are directly performed on this set of invariants. Geometric distortions are generally simple and effective attacks for many watermarking methods. They can make detection and extraction of the embedded watermark difficult or even impossible by destroying the synchronization between the watermark reader and the embedded watermark. They also shown how the moments

can be exploited for estimating the geometric distortion parameters in order to permit watermark extraction.

The proposed watermarking scheme is robust to a wide range of attacks: geometric distortion, filtering, compression, and additive noise. The major contribution of this paper relies on two aspects. The first one is the derivation of a set of affine invariants based on Legendre moments. Those invariants can be used for estimating the affine transform coefficients applied to one image. The second one is the use of these affine Legendre moment invariants for watermark embedding, detection and extraction. It was shown that the proposed method is more robust than others based on geometric moments.

One weak point of this algorithm is that the watermark detection is considered as a 1-bit watermarking system since the distance between the affine invariants and the threshold is used. However, the proposed detection approach could be extended to a multi-bit watermarking scheme by making use of spread spectrum techniques for example. Another limitation of the proposed algorithm is that it is not robust to image cropping and histogram equalization, a common problem for the moment-based watermark algorithms.

2.4 J.-S. Tsai, W.-B. Huang, and Y.-H. Kuo, "On the selection of optimal feature region set for robust digital image watermarking," IEEET trans. Image Process., vol. 20, no. 3, pp. 735–743, Mar. 2011.

In this paper a novel feature region selection method for robust digital image watermarking is proposed. This method aims to select a nonoverlapping feature region set, which has the greatest robustness against various attacks and can preserve image quality as much as possible after watermarked. It first performs a simulated attacking procedure using some predefined attacks to evaluate the robustness of every candidate feature region. It then adopts a track-with-pruning procedure to search a minimal primary feature set which can resist the most predefined attacks. In order to enhance its resistance to undefined attacks under the constraint of preserving image quality, the primary feature set is then extended by adding into some auxiliary feature regions.

This work is formulated as a multidimensional knapsack problem and solved by a genetic algorithm based approach. The experimental results for Stirmark attacks on some benchmark images support their expectation that the primary feature set can resist all the predefined attacks and its extension can enhance the robustness against undefined attacks. Comparing with some well-known feature-based methods, the proposed method exhibits better performance in robust digital watermarking.

A novel method based on the simulated attacking approach and the GA-based MDKP(multidimensional knapsack problem) solving procedure is developed to select the most adequate feature regions for robust digital image watermarking under the constraint of preserving image quality. Compared with other feature-based watermarking methods, the robustness against various attacks is significantly improved by the proposed method, and the image quality after watermarking is still preserved. The proposed method consumes too much computation time in measuring the robustness of feature regions due to the simulated attacking.

2.5 N. K. Kalantari, S. M. Ahadi, and M. Vafadust, "A robust image watermarking in the ridgelet domain using universally optimum decoder," IEEE Trans. Circuits Syst. Video Technol., vol. 20, no. 3,pp 396–406.

In this paper a robust image watermarking scheme in the ridgelet transform domain is proposed. Due to the use of the ridgelet domain, sparse representation of an image which deals with line singularities is obtained. In order to achieve more robustness and transparency, the watermark data is embedded in selected blocks of the host image by modifying the amplitude of the ridgelet coefficients which represent the most energetic direction. Since the probability distribution function of the ridgelet coefficients is not known, they propose a universally optimum decoder to perform the watermark extraction in a distribution independent fashion. Decoder extracts the watermark data using the variance of the ridgelet coefficients of the most energetic direction in each block. Furthermore, since the decoder needs the noise variance to perform decoding, a robust noise estimation scheme is proposed.

The proposed method shows outstanding robustness against common attacks, especially additive white noise and JPEG compression. Using the ridgelet domain, a sparse representation of images was obtained. The watermark signal was embedded into the ridgelet coefficients, which represent the most energetic direction, by simply modifying their amplitude according to the watermark data. Due to the useful properties of the ridgelet transform, random noise cannot produce significant coefficients which lead to robustness of our watermarking scheme. Furthermore, in order to obtain maximum robustness, the decoder was optimized by considering Gaussian noise attack. The varience ratio for extracting the watermark data is used , the decoder was independent of host signal distribution. This was a good achievement, since the distribution of ridgelet coefficients is not well known. Thus, the decoder always works near optimum point. Furthermore, a robust noise variance estimation method was proposed to be used in watermark extraction procedure.

2.6 L. Xin-Wei, G. Bao-Long, L. Lei-Da, and S. Hong-Xin, "A new histogram based image watermarking scheme resisting geometric attacks," in Proc. 5th Int. Conf. Inf. Assurance Secur., Aug.2009, pp. 239–242.

In this paper, they proposed a new histogram modification scheme considering the visual quality of the watermarked image. They use the mean pixel value of divided blocks to calculate histogram and the mean square error to select blocks to be modified based on HVS. They obtained a good trade-off between robustness to geometric attacks and common image processing attacks by adjusting the block size. This is complete embedding scheme and the reverse of this is done in decoding scheme. Finally, the complete embedding and extracting algorithms are given. The proposed approach has an excellent robustness against geometric attacks and some normal attacks, such as adding noise and JPEG compression. In the proposed scheme, they have presented two optimization methods based on Xiang et al."s method from histogram modification and pixel modification respectively.

2.7 S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 6, pp. 777–790, Jun. 2008.

In this paper, they presented an image watermarking scheme by the use of two statistical features (the histogram shape and the mean) in the Gaussian filtered low-frequency component of images.

The features are:

1) Mathematically invariant to scaling the size of images
2) Independent of the pixel position in the image plane
3) Statistically resistant to cropping
4) Robust to interpolation errors during geometric transformations, and common image processingoperations .

Watermark resistance to geometric attacks is an important issue in the image watermarking community. Most countermeasures proposed in the literature usually focus on the problem of global affine transforms such as rotation, scaling and translation (RST), but few are resistant to challenging cropping and random bending attacks (RBAs). The main reason is that in the existing watermarking algorithms, those exploited robust features are more or less related to the pixel position.

The watermarking system provides a satisfactory performance for those content-preserving geometric deformations and image processing operations, including JPEG compression, lowpass filtering, cropping and RBAs. A key-based PN sequence is successfully inserted by modifying the histogram shape, which is computed from the low-frequency component of Gaussian filtered images by referring to the mean. The watermark can be detected without knowledge of original images by sharing the exploited private key in the detector. However, the histogram-based watermarking have its limitation for histogram equalization since this operation will distort the histogram shape much. Histogram equalization is a useful technique for improving image contrast, but its effect is too severe for many purposes. In addition, the watermark may suffer from a key estimation attack since the length of the exploited PN sequence is limited.

2.8 J. F. Lichtenauer, I. Setyawan, T. Kalker, and R. L. Lagendijk,"Exhaustive geometrical search and the false positive watermark probability," detection Proc. SPIE, Secur. Watermarking Multimedia Contents V,vol. 5020, pp. 203–214, Jun. 2003.

This paper considers the more important problem of false positives, in addition to the computational cost required for this method. One way of recovering watermarks in geometrically distorted images is by performing a geometrical search. The maximal number of detections that can be performed in a geometrical search is bounded by the maximum false positive detection probability required by the watermark application.

False positive detection probability, in the correlation-based watermarking scheme we used in this research, is dependent on image content and detection keys. Because of these dependencies, varying over transforms only, while keeping the other factors constant, like in a normal geometrical search, gives a different false positive detection probability in a geometrical search for each choice of the constant factors on which the watermarking scheme is dependent.

It is shown in the paper that image and key dependency in the watermark detector leads to different false positive detection probabilities for geometrical searches for different images and keys. Furthermore, the image and key dependency of the tested watermark detector increases the random-image-random-key false positive detection probability.

2.9 P. Dong, J. G. Brankov, N. Galatsanos, and Y. Yang, "Geometric robust watermarking based on a new mesh model correction approach," in Proc.IEEE Int. Conf. Image Process.,Jun.2002,pp.493-496.

In this paper, they presented a watermarking scheme based on a new deformable

mesh model to combat geometric attacks. The distortion is corrected using the distortion field (DF) estimated by minimizing the matching error between the meshes of the original and attacked image. A CDMA watermarking method is used for testing the proposed method, which embeds a multi-bit signature in the DCT domain and uses mesh model correction to achieve robustness.

In this paper they proposed a new objective function to estimate the DF. This objective function consists of two terms. The first term captures the matching error between the original and the attacked watermarked image, and the second term captures the regularity of the DF. This new objective function forces the smoothness of the DF, instead of mesh regularity, so that it can capture effectively the distortion in the attacked image. The estimated DF is then used for distortion compensation. They applied a CDMA based multi-bit watermarking scheme for the embedder , by virtue of its property of high- robustness to common signal processing operations.

2.10 N. K. Kalantari, S. M. Ahadi, and M. Vafadust, "A robust image watermarking in the ridgelet domain using universally optimum decoder,"IEEE Trans. Circuits Syst. Video Technol., vol. 20, no. 3,pp. 396–406, Mar. 2010.

This paper investigates a non – blind method to reverse the effect of local geometric distortions, in order to recover the signature from image close to the original one . Another non – blind method with the same objective is introduced, making use of representative feature points at multiple resolutions.

They presented in this paper a compensation technique allowing to retrieve a watermark in an image from the original image, or its edges. For this they use 2D mesh, in order to compensate parts of geometric distortion that could be introduced by softwares such as Stirmark. In order to illustrate the usefulness of the compensation on attacked images, they used two watermarking techniques : classical

spread spectrum algorithm proposed by Cox etal. (the watermark is embedded into a selected set of DCT coefficients) and a wavelet based watermarking technique.

In this paper, geometric attacks compensation algorithm has been presented. They have shown that it allows to retrieve the watermark from an attacked image, if this is watermarked in its DCT (spread spectrum technique) or its DWT (significant wavelet coefficients quantization) representation.

2.11 N. F. Johnson, Z. Duric and S. Jajodia, "Recovery of watermarks from distorted images,"in Proc. 3rd Int. Workshop Inf.Hiding,1999,pp.318-332.

In this paper authors have described a method for the recovery of original size and appearance of images based on the concept of identification marks ("fingerprints"); the method does not require the use of the "original" image, but only a small number of salient image points. Using this method, it is possible to recover original appearances of distorted images. The restored image can be used to recover embedded watermarks.

Digital works are subject to illicit copying and distribution. Many owners wish for some means of identifying ownership and copyright. Digital watermarks can fulfill this role and provide a means to identify and track digital works. However, embedded watermarks may fail to be recognized due to accidental corruption or attack by cropping and/or affine distortions (e.g., rotation, scaling, and blurring) . This hampers the ability to locate and identify watermarked images over distributed networks such as the Internet.

In this paper, they introduced alternative methods for image recovery, based on inherent features within images that can be used to "fingerprint" images. These identification marks can be applied to locate images and recover image size and aspect from distorted images. The proposed methods do not rely on embedded information and can be used to recover images distorted by various geometric transformations.

2.12 S. Pereira, J. J. K. O. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun,"Template based recovery of Fourier-based watermarks using log-Polar and log-log maps," in Proc. IEEE Int. Conf. Multimedia Comput. Syst., Jul. 1999, pp. 870–874.

This paper describes a method for the secure and robust copyright protection of digital images. Digital watermarks have been proposed as a method for discouraging illicit copying and distribution of copyrighted material. The authors presented an approach for embedding a digital watermark into an image using the fast Fourier transform. To this watermark is added a template in the Fourier transform domain to render the method robust against rotations and scaling, or aspect ratio changes.

The proposed method in the text that follows consists of embedding a watermark in the FFT domain. The watermark is composed of two parts, a template and a spread spectrum signal containing the information or payload. The template contains no information in itself, but is used to detect transformations undergone by the image. Once detected, these transformations are inverted and then the spread spectrum signal is decoded. The spread spectrum signal contains information such as the owner of the image, a serial number and perhaps flags which indicate the type of content e.g. religion, pornography, or politics. This can be useful for indexing images or even for tracking pornography on the web.

WORK DONE

3.1 Introduction

Watermarking is a process that embeds important data related to image, audio, video into a multimedia object such that the important data can be detected or extracted later to make an assertion about the object. It is a process of embedding the secret or special information which a user wants to hide and it is called as watermark.

Various techniques of watermarking are available. With this different techniques the watermark image can embedded in the host image by either making it visible or invisible. Invisible watermarking is more robust and reliable as compared to the visible watermarking because the secret element or information cannot be perceived due to the limitations of Human Visual System (HVS) which makes it secure and reliable from the unauthorized users. Human perception system can distinguish 32 gray intensity levels out of the 256 intensity levels which explains the fact that a human eye can distinguish between intensity values of 34 and 43 but cannot distinguish between the intensity values of 34 and 36 and they will appear to have same gray shade.

In this work, a invisible watermarking technique is carried out in the embedding process and the extraction of the inserted watermark is done in the decoding process .Several attacks are introduced in the decoding process and decoding process is robust or not against this attacks is find out.

3.2 Watermark embedding process

The watermark embedding process of the proposed method is shown in Fig. 1. It consists of four steps: Gaussian filtering, histogram construction, pixel group selection, and HFCM based watermark embedding.

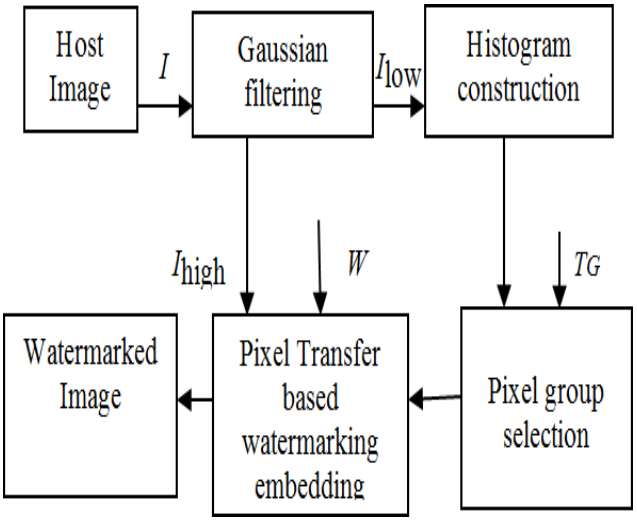


Fig-3.1 Block diagram of watermark embedding process

Gaussian Filtering:

The host gray scale image I is preprocessed by 2-D Gaussian low pass filter.

$$F(x, y, \sigma) = \frac{1}{2\Pi\sigma^2} e^{\frac{-x^2 + y^2}{2\sigma^2}} \quad (1)$$

where (x , y) indcates the pixel position and σ is the standard deviation of the distribution, which is usually chosen as σ = 1.

The filtered image I_{low} can be shown as

$$I_{low}(x , y) = F(x,y,\sigma)*I(x,y) \quad (2)$$

I_{high} is the high frequency component which is removed from host image by the Gaussian filtering,it follows:

$$I_{high}(x,y) = I(x,y) - I_{low}(x , y) \quad (3)$$

Thus, the host gray scale image is separated into two parts that are I_{low} and I_{high} . The size of the Gaussian mask F is often chosen using expression (2kσ + 1) × (2kσ + 1), where k is a positive integer.

Histogram Construction:

We assumed that the filtered image I_{low} has K gray levels, e.g., an 8-bit gray scale image has K = 256 gray levels, which is ranging from 0 to 255. The histogram of an image is the number of pixels versus the gray level values. To select S gray levels from the K available gray levels we have calculated the mean of the histogram, where

$$K / 2 \leq S < K \tag{4}$$

Thus the histogram of an image I_{low} is given by

$$Hs = \{ hs(Ki) \mid i=1,2,\ldots,S \} \tag{5}$$

Where hs(Ki) is the number of pixels corresponding to gray level Ki.

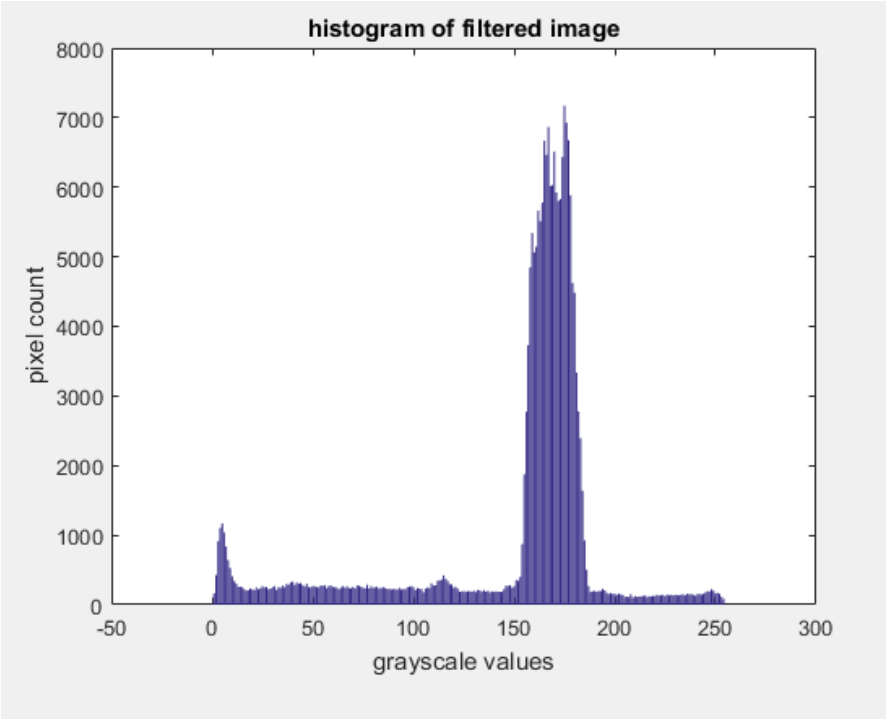


Fig-3.2 Histogram of filtered image

Fig. 2 shows the histogram of filtered image. The x-axis denotes gray scale values and y-axis denotes pixel counts of this gray scale values. The mean obtained here is 820.3125 ≈ 820 and the number of gray scale values which have mean less than or equal to 820 are 219. But when 219 gray scale values are taken for further processing then the filtered image gets blur. To avoid this blurring of the filtered image the three gray scale values are not considered and finally 216 values are selected for the formation of bins i.e S = 216 .

Pixel group selection :

After histogram construction Hs , we form bin. One can form bins in total as,

$$M_B = [\ S/L_B\ ] \tag{6}$$

Assume $L_B = 3$,

$$M_B = [\ 216/3\ ]$$

$$M_B = 72$$

The number of pixels in the ith bin is

$$h_B(i) = h_s(K(i-1).L_B+1) + h_s(K(i-1).L_B+2) + \ldots + h_s(Ki.L_B) \quad (7)$$

where $i = 1,2,\ldots, M_B$.

After this we take each two neighboring bins to form a group which will produce $[M_B/2]$ i.e $[72/2] = 36$ groups.

The two bins (Bin_1 and Bin_2) contains $h_B(2i-1)$ and $h_B(2i)$ pixels. Thus, number of pixel in the ith bin is

$$h_G(i) = h_B(2i-1) + h_B(2i),\ i = 1,2,\ldots,[M_B/2] \quad (8)$$

where $i = 1,2,\ldots, [M_B/2]$.

Pixel Transfer based watermark embedding :

Let us assume that $W1,W2,\ldots,W_{LW}$ are the watermark bits to be embedded into the L_W chosen groups, respectively. The watermark image size is 5 × 5 i.e 25 and the chosen groups are 36 . Each chosen group, say the i th group have two bins: Bin_1 have $h_B(2i-1)$ pixels and Bin_2 have $h_B(2i)$ pixels. Then, one can embed the watermark bit wi into the ith chosen group using the following embedding rule:

$$h_B(2i-1) / h_B(2i) \geq 2, \quad \text{if } wi = 1 \quad (9)$$

$$h_B(2i-1) / h_B(2i) \leq ½ \quad \text{if } wi = 0 \quad (10)$$

The above rule says that if wi = 1, a certain number of pixels (say N1) should be transferred from Bin_2 to Bin_1 such that $h_B(2i-1) \geq 2h_B(2i)$. Likewise, if wi = 0, some pixels (say N0) need to be transferred from Bin_1 to Bin_2 such that $h_B(2i-1) \leq (1/2)h_B(2i)$.

The minimum N0 and N1 are

$$N0 = 2h_B(2i - 1) - h_B(2i) / 3 \quad (11)$$

$$N1 = 2h_B(2i) - h_B(2i - 1) / 3 \quad (12)$$

We proposed a new pixel transfer approach to reduce the extent of pixel movements. The L_B gray levels in Bin_1 are $K_{(i-1)\cdot LB+1}$, $K_{(i-1)\cdot LB+2}$, $K_{i\cdot LB}$ and those in Bin_2 are $K_{i\cdot LB+1}$, $K_{i\cdot LB+2}$,...,$K_{(i+1)\cdot LB}$ .The numbers of pixels at these gray levels are $N_{K(i-1)\cdot LB+1}$, $N_{K(i-1)\cdot LB+2}$,…, $N_{K(i+1)\cdot LB}$ respectively. Our approach considers the following two cases:

1) Case 1:

If $N_{Ki\cdot LB+1} \geq N_0$, move N_0 pixels from gray level $K_{i\cdot LB+1}$ to gray level $K_{i\cdot LB+2}$ within Bin_2. Then, select N_0 pixels from Bin_1 as follows.

a) If $N_{Ki\cdot LB} \geq N_0$, then choose all N_0 pixels from gray level $K_{i\cdot LB}$.

b) If $N_{Ki\cdot LB} \leq N_0$ then choose $N_{Ki\cdot LB}$ pixels from gray level $Ki\cdot LB$ and the remaining N_0 - $N_{Ki\cdot LB}$ pixels are chosen from the other gray levels in Bin_1.

The pixels selected in Bin_1 are moved to the gray level $Ki\cdot L_B+1$ in Bin_2.

2) Case 2:

If $N_{Ki\cdot LB+1} < N_0$, move all $N_{Ki\cdot LB+1}$ pixels from gray level $Ki\cdot L_B+1$ to gray level $Ki\cdot L_B+2$. Then, select N_0 pixels from the L_B gray levels in Bin_1 in the way described in Case 1. Among these selected pixels, move the first $N_{Ki\cdot LB+1}$ pixels to gray level $Ki\cdot LB+1$ and the remaining $N_0 - N_{Ki\cdot LB+1}$ pixels to gray level $K_{i\cdot LB+2}$

Fig-3.3 Host image

Fig-3.4 Filtered image

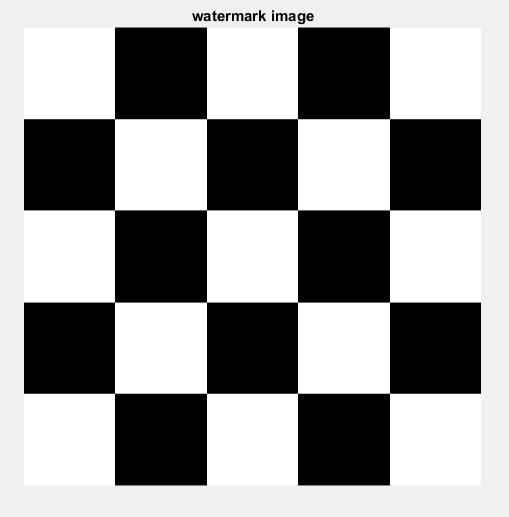


Fig-3.5 Watermark image

Fig-3.6 Watermark embedded image

3.3 Watermark decoding process

Fig. 2 represent block diagram of watermark decoding method. It consists of three steps : Histogram construction, identification of watermarked groups and watermark extraction.

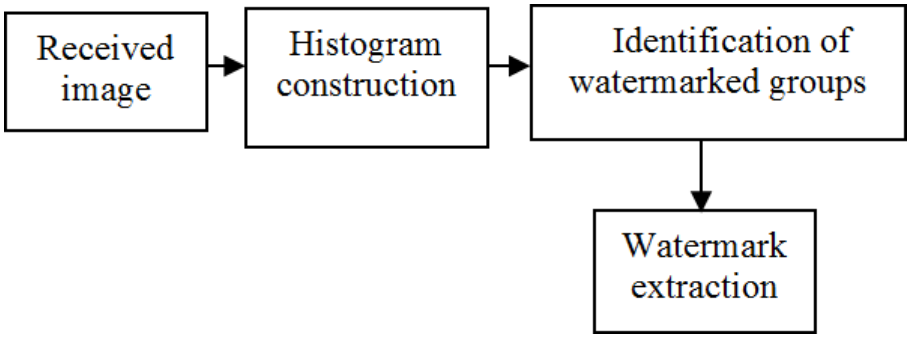


Fig-3.7 Block diagram of watermark decoding process

Histogram Construction:

Based on the mean, we finds the S gray levels K1, K2,.., KS used for watermark embedding, from the K possible gray levels. Then, construct the histogram of I „low, denoted as H‟S.

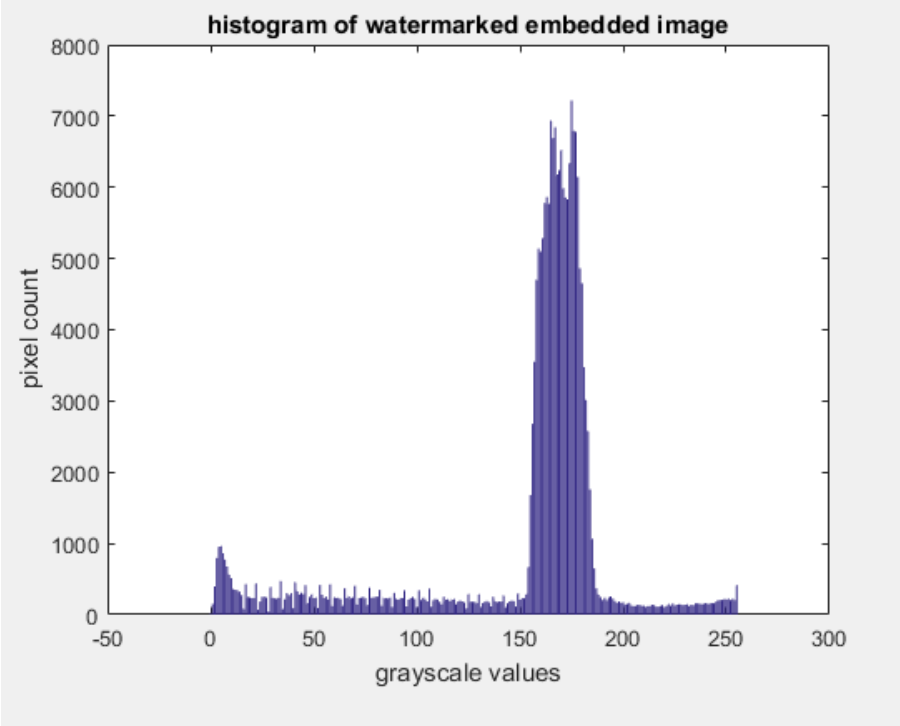


Fig-3.8 Histogram of watermarked embedded image

Fig. 8 shows the histogram of watermarked embedded image. The gray scale values here are same as that of the embedding process that is S = 216. But there is difference in the pixel values of this selected gray scale values as compared to the embedding process.

Identification of Watermarked Groups :

The process of group selection is same which is carried in the embedding process. Initially we have to find the bins. To form a bin take each LB neighboring gray levels in H‟S and take each two neighboring bins as a group. Then number of pixels are calculated of this selected bins as h‟B(i). Further, we take each two neighboring bins to form a group and the number of pixels in each group is calculated as h‟G(i) .

Watermark Extraction:

For the i th watermarked group, h‟B(2i − 1) and h‟B(2i) denote the number of pixels in the first bin and h‟B(2i) denote the number of pixels in the the second bin, respectively.

If h‟B (2i − 1) / h‟B (2i) ≥ 1, the extracted watermark bit is 1; otherwise, watermark bit 0 is extracted. There are 13 groups which have ratio of pixel values greater than or equal to one , it means 13 watermark bits are one. The remaining 12 groups have ratio of pixel values less than one , it means 12 watermark bits are zero .

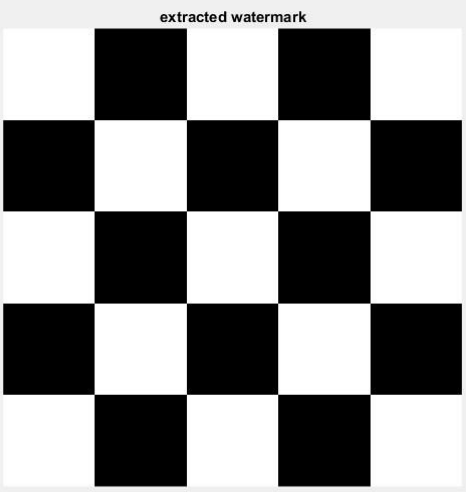


Fig-3.9 Watermarked embedded image **Fig-3.10 Extracted Watermark image**

RESULTS AND DISCUSSION

4.1 Simulation Results

The host image birdgray.jpg of size 350 × 600 is taken as the input image and user define watermark image of size 5 × 5 is taken respectively. The simulation of algorithm is carried out using these images and a mean is found which is later used for the grouping of bins for the insertion of watermark image in the embedding process. The embedding and extraction process are simulated in MATLAB R2016a.

350x600 uint8

	1	2	3	4	5	6	7	8	9	10
1	77	104	110	111	111	113	113	113	113	111
2	103	140	149	149	150	151	151	151	150	150
3	109	149	157	158	159	159	160	160	159	158
4	110	149	157	159	159	160	161	160	160	159
5	110	149	157	159	159	160	161	160	160	159
6	110	149	157	159	159	160	161	160	160	159
7	110	149	157	159	159	160	160	160	160	159
8	110	149	157	158	159	159	159	160	160	160
9	111	149	157	158	158	158	158	159	160	160
10	111	149	158	158	158	157	157	158	160	161
11	111	150	158	158	158	158	158	159	160	161
12	111	150	158	158	158	158	158	159	160	161
13	111	150	158	158	158	158	158	159	161	162
14	113	151	159	159	159	159	159	160	161	162
15	113	152	161	161	161	160	160	161	162	163

Fig-4.1 Host image pixel values (image size 350 X 600)

5x5 double

	1	2	3	4	5
1	1	0	1	0	1
2	0	1	0	1	0
3	1	0	1	0	1
4	0	1	0	1	0
5	1	0	1	0	1

Fig-4.2 Watermark image pixel values (image size 5 X 5)

350x600 uint8

	1	2	3	4	5	6	7	8	9	10
1	157	157	158	159	159	161	162	162	160	159
2	157	157	159	159	159	160	161	161	159	159
3	157	158	158	159	159	160	161	161	159	159
4	157	158	158	159	159	160	161	161	160	159
5	157	158	158	159	159	160	161	161	160	159
6	157	158	158	159	159	160	161	161	160	159
7	157	158	158	159	159	160	161	161	160	159
8	157	158	158	159	159	160	161	161	160	160
9	158	158	158	158	158	158	158	159	161	161
10	159	159	159	158	158	157	157	158	161	161
11	160	159	159	159	158	158	158	159	161	161
12	159	159	159	158	158	158	158	159	162	162
13	159	158	158	158	158	158	158	159	162	162
14	161	159	159	159	159	159	159	160	163	163
15	162	162	162	161	161	160	160	161	163	163

Fig-4.3 Watermark Embedded image pixel values (image size 350 X 600)

4.2 Watermarking Attacks Results

For the robustness analysis of the discussed algorithm, the algorithm was attacked with various types of watermarking attacks. The effectiveness of the algorithm is measured in terms of quantities of Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM) and Bit Error Rate (BER) to quantify how similar the watermark image, retrieved from the attacked host image, is in comparison to the original watermark image.

PSNR is most commonly used to measure the quality of reconstruction of lossy compression. The signal in this case is the original data, and the noise is the error introduced by various watermarking attacks. PSNR is an approximation to human perception of reconstruction quality.

SSIM is used for measuring the similarity between two images. The difference with respect to PSNR is that these approach estimate absolute errors; on the other hand, SSIM is a perception-based model that considers image degradation as perceived change in structural information, while also incorporating important perceptual phenomena, including both luminance masking and contrast masking terms.

Bit error rate is defined as the rate at which errors occur in an image. This can be directly translated into the number of errors that occur in an pixels of an image. The bit error ratio is the number of bit errors divided by the total number of transferred bits during a studied time interval.

The various commands in MATLAB 2016a used for PSNR, SSIM and BER are:-

peaksnr = psnr(a, ref)

ssimval = ssim(a, ref)

For BER there is no direct command available, so we have created a function as „biter".

out = biter(a, ref)

where, „a" is an attacked embedded watermark image and „ref" is the host image.

When attack is done on the embedded watermark image the size of the image gets alter in some attacks. Thus, in these cases of attacks the PSNR and SSIM cannot be computed, whereas BER will only be calculated when the size of an attacked image is greater than or equal to the host image.

The process of insertion of watermark is based on the group selection criteria. The gray scales values of an image which are grouped are selected according to the mean of the filtered image from the histogram construction. In our proposed algorithm there is no need of shifting the histogram of an image and hence the extracted watermark is same as the inserted watermark. The instance of watermark is shown below when it is not extracted same as the inserted watermark.

Fig-4.4 Histogram shifted image

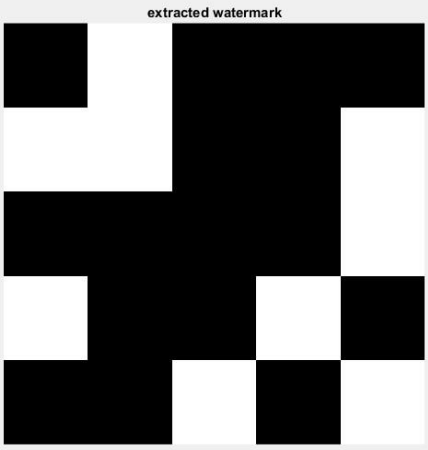


Fig-4.5 Extracted Watermark image from the Histogram shifted image

Fig-4.6 Without any attack image

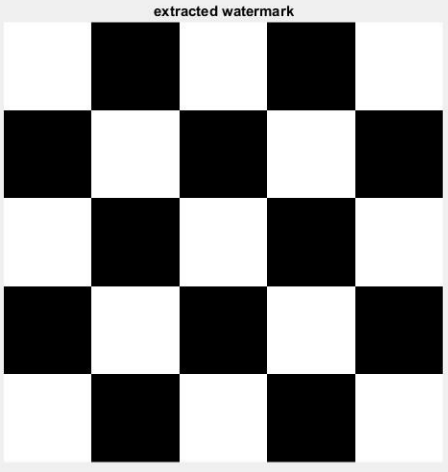


Fig-4.7 Extracted Watermark image from without any attack image

Now our embedded watermarked image undergoes certain attacks.

Fig-4.8 Rotating an image by 35º

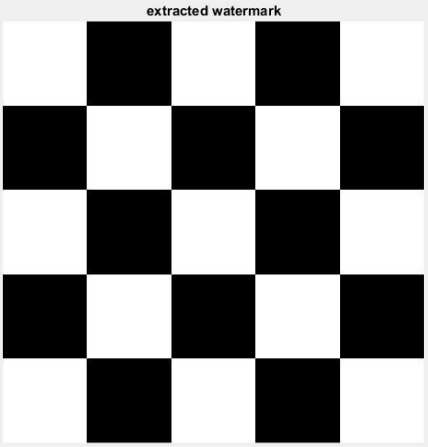


Fig-4.9 Extracted Watermark image from the rotated image

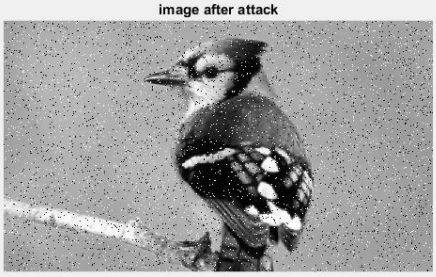


Fig-4.10 Salt and pepper attack

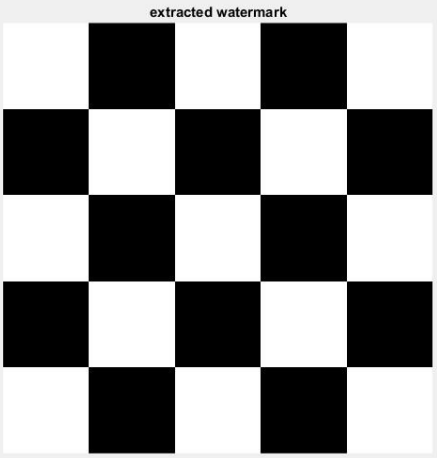


Fig-4.11 Extracted Watermark image from the salt and pepper image

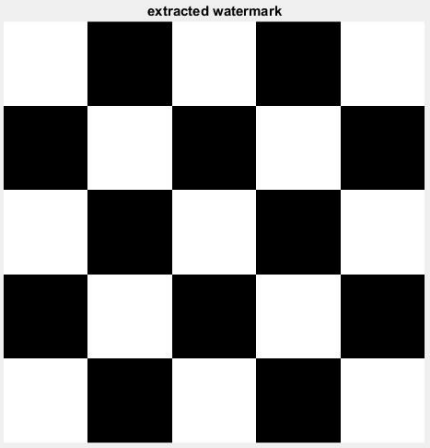
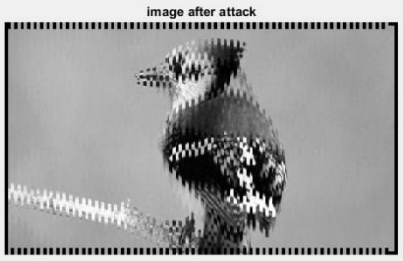


Fig-4.12 Scaling an image by 0.7

Fig-4.13 Extracted Watermark image from the scaled image



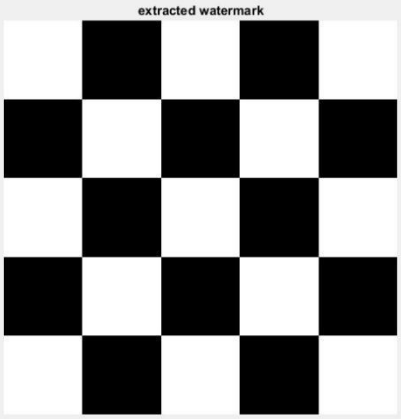


Fig-4.14 Random bending attack

Fig-4.15 Extracted Watermark image from the RBA image

Fig-4.16 Attack by cropping an image

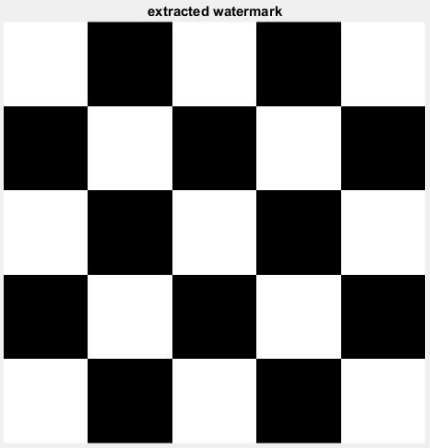


Fig-4.17 Extracted Watermark image from the cropped image

Table-4.1 Analysis of attacks

ATTACKS	EMBEDDED WATERMARK IMAGE SIZE	PSNR	SSIM	BER
HISTOGRAM SHIFTED IMAGE	350 × 600	13.6902	0.6245	0.9915
WITHOUT ATTACK	350 × 600	36.1810	0.9866	0.2364
Rotation an image by 35º	631 × 693	-	-	0.9820
Salt and Pepper attack	350 × 600	18.1367	0.2667	0.2745
Scaling an image by 0.7	245 × 420	-	-	-
Random bending attack	360 × 610	-	-	0.8522
Attack by Cropping an image	321 × 551	-	-	-

SUMMARY AND CONCLUSIONS

5.1 Summary

In this work, a watermarking algorithm applicable on grayscale images has been build. The initial stage of approach was accomplished by building the watermarking embedding process and finally followed by watermarking decoding process. The robustness of the watermarking algorithm is verified by attacking the watermarked image with various types of attacks. The respective results are obtained in MATLAB R2016a.

5.2 Conclusion

Thus, we can conclude that the proposed algorithm is robust against different attacks. By attacking the watermarked image with various types of attacks we got the same watermark image in the decoding process which was inserted during the embedding process. Thus we can conclude, the proposed algorithm is robust because the extracted watermark image is same as that of the inserted watermark image when various attacks are introduced.

5.3 Future Work

The proposed algorithm is tested on gray scale images and against various image processing attacks in the MATLAB R2016a for checking the robustness of the algorithm against this watermarking attacks. The modification can be done in the algorithm for direct application on the colour images and there will be no need of changing the composition of 3D colour images into 2D gray scale images for application of the algorithm.

Literature Cited

References

[1] Tianrui Zong, Young Xiang, Wanlei Zhou and Gleb Beliakov," Robust Histogram Shape-Based Method for Image Watermarking" IEEE Transactions on circuits and system for video technology,vol.25,No.5,717-729, 2015.

[2] L. Wang, H. Ling, F. Zou, and Z. Lu, "Real-time compressed domain video watermarking resistance to geometric distortions," IEEE MultiMedia, vol. 19, no. 1, pp. 70–79, Jan. 2012.

[3] H. Zhang et al., "Affine Legendre moment invariants for image watermarking robust to geometric distortions," IEEE Trans. Image Process.,vol. 20, no. 8, pp. 2189–2199, Aug. 2011.

[4] J.-S. Tsai, W.-B. Huang, and Y.-H. Kuo, "On the selection of optimal feature region set for robust digital image watermarking," IEEET trans. Image Process., vol. 20, no. 3, pp. 735–743, Mar. 2011.

[5] N. K. Kalantari, S. M. Ahadi, and M. Vafadust, "A robust image watermarkin in the ridgelet domain using universally optimum decoder," IEEE Trans. Circuits Syst. Video Technol., vol. 20, no. 3,pp 396–406.

[6] L. Xin-Wei, G. Bao-Long, L. Lei-Da, and S. Hong-Xin, "A new histogram based image watermarking scheme resisting geometric attacks," in Proc. 5th Int. Conf. Inf. Assurance Secur., Aug.2009, pp. 239–242.

[7] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 6, pp. 777–790, Jun. 2008.

[8] J. F. Lichtenauer, I. Setyawan, T. Kalker, and R. L. Lagendijk, "Exhaustive geometrical search and the false positive watermark probability," detection Proc. SPIE, Secur. Watermarking Multimedia Contents V,vol. 5020, pp. 203–214, Jun. 2003.

[9] P. Dong, J. G. Brankov, N. Galatsanos, and Y. Yang, "Geometric robust watermarking based on a new mesh model correction approach," in Proc.IEEE Int. Conf. Image Process.,Jun.2002,pp.493-496.

[10] N. K. Kalantari, S. M. Ahadi, and M. Vafadust,"A robust image watermarking in the ridgelet domain using universally optimum decoder,"IEEE Trans. Circuits Syst. Video Technol., vol. 20, no. 3,pp. 396–406, Mar. 2010.

[11] N. F. Johnson, Z. Duric and S. Jajodia, "Recovery of watermarks from distorted images,"in Proc. 3rd Int. Workshop Inf.Hiding,1999,pp.318-332.

[12] S. Pereira, J. J. K. O. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun,"Template based recovery of Fourier-based watermarks using log- Polar and log-log maps," in Proc. IEEE Int. Conf. Multimedia Comput. Syst., Jul. 1999, pp. 870–874.

List of publication

Sr. No.	Authors	Title of Paper	Name of International Conference	Status	Place and date of Conference
1	Apoorva Sharma Swati Nitanaware	Image Watermarking using Robust Histogram Shape Method	4th IEEE International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS-17)	Presented	Coimbatore, Tamilnadu 17-18 March 2017