Image Watermarking using Wavelet Denoising Method

Kalpana Bhelotkar, Sandeep B. Patil

Abstract*— Robust image watermarking aims to embed invisible information, typically for copyright protection applications, in images in a way that the watermark is robust against various image processing attacks. Such attacks can be divided into signal processing and geometric attacks leading to different requirements for achieving robustness against attacks. This thesis investigate approaches to robust image watermarking focusing on the type of watermarking techniques termed as "second generation watermarking". This class of watermarking schemes increases robustness against geometric attacks by including the use of the image's perceptual features into the marking/detection process. Additional focus is put on the wavelet transform and its properties relevant for applications in robust image watermarking.

Keywords*— Digital Image Watermarking, Singular Value Decomposition, Watermark Embedding Algorithm, Watermark Extracting Algorithm.

I. INTRODUCTION

Computers and the Internet have long made their way into private living rooms, and activities of daily life, like writing letters, shopping, listening music and watching movies now involve computing technology. The way computers deal with data digitized representation introduces new opportunities but also new problems: finding a reasonable compromise between user-friendliness and security is often difficult, "goods" like multimedia objects are technically a bunch of bits and bytes that can easily be perfectly copied and even redistributed, digital images can easily be manipulated making them unsuitable as proofs in criminal cases etc. There are various concepts aiming to solve some of these problems including legal protection, technical standards, digital rights management and copyright protection. For multimedia objects, like images, videos and sound, two of the above problems apply in particular: the question of an object's authenticity, i.e. originality, and protection of copyright against pirating, or false ownership claims. Digital watermarking plays an increasingly important role for proving authenticity and copyright protection. Most multimedia formats do not introduce any restriction on copying or manipulating multimedia objects; and while the Internet is an ideal medium for selling digital goods it also makes redistribution of pirated copy is very easy. Digital watermarking can be used to insert invisible data into an object helping to track down pirate copies and to prove rightful ownership in a dispute. In principle, watermarking technologies can be applied to any kind of multimedia object, however to achieve the best possible results schemes are normally optimized on a particular medium.

Manuscript Received on July, 2013.

Kalpana Bhelotkar, ET & T Dept.., C.I.T. Rajnandgaon, Rajnandgaon (C.G.), India.

Sandeep B. Patil, ET & T Dept., SSCET Bhilai, Bhilai(C.G.), India.

The term "watermark" has been known long before the age of computing: watermarks were found on bank notes to make falsification difficult or on writing paper to add an individual taste or corporate identity. On computers, such applications are possible, too: in 1994, the German software company Star Division distributed free copies of their word processor Star Writer to visitors on the Hanover CeBit fair; the copies were fully functional, only that when printing documents from within the application, a watermark would be printed as the background of the document's pages. Other common applications for watermarks on computers include proof of rightful ownership and authentication for multimedia objects like images. Since multimedia objects are digital representations of analogue data (like sound, photos, movies) they tolerate some amount of manipulation as long as some rules are obeyed. If some pixels' intensities in an image are changed subtly, the human eye is unlikely to notice this, yet these changes can carry information visible to the respective detection software. Fig. (1) shows a principle of digital image watermarking system setup.

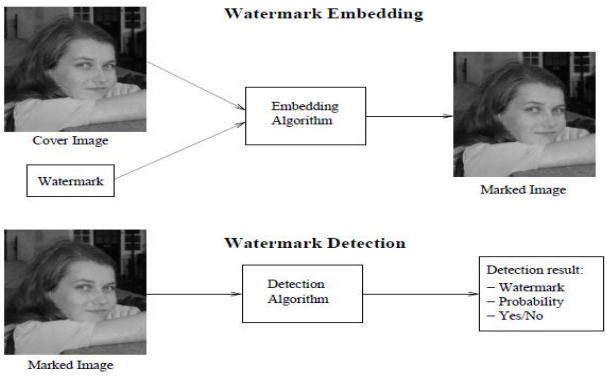

Fig. (1) Principle Image Watermarking Framework

In many cases there is an additional data item necessary for embedding or detection, like a secret key. Also, the kind of detection result obviously depends on the watermarking system's purpose and design in some cases the presence of a known watermark pattern is detected, in others a message of some kind (text, or even multimedia contents like images, audio etc.) is read.

II. LITERATURE SURVEY

Watermarking can serve various purposes; hence there are a number of different types of watermarks. In the literature (e.g. in, we find two main applications for digital image watermarking:

A. Content Authentication

The watermark is used to prove authenticity, i.e. ensure that the image has not been manipulated in any way.

This is useful whenever the originality of an image is important, like the protection of historical images and evidence before courts.

B. Proof of Rightful Ownership

The watermark is used to support claims on rightful ownership of an image. It can also help to detect unauthorized copies and by embedding serial numbers to track down the licensee from who a pirate copy originated.

C. Fragile Watermarks

The watermark is destroyed by any manipulations of the image. Therefore originality of the image is established if the watermark can still be read/detected. The watermark can be seen as a seal protecting the object's content, but unlike in the "real world" it does not restrict from read-only access.

D. Robust Watermarks

The watermark survives a reasonable amount of image manipulation. The term "reasonable" means that the image quality after such manipulation should be high enough to maintain the value of image value to user. Robust watermarks used for tracking down pirated copies are usually embedded per customer or group of customers; such marks are often referred to as fingerprints in the literature. Technically, this second category is the greater challenge since due to the nature of multimedia objects it is much easier to apply significant yet imperceptible changes than the other way round. Both kinds of watermarks must at the same time operate without causing perceptible distortion in the object; the actual thresholds of what is acceptable depend to a large extent on the application.

Already in 1998, Petitcolas et al. introduced the so-called Stir-Mark benchmark for copyright marking schemes on images which consisted of a combination of different image manipulation operations and was so powerful that the vast majority of schemes known at that time were unable to withstand it. The authors claimed that watermarking systems not robust against this benchmark should be considered unacceptably and easy to break. There have been different approaches to make copyright marking systems more robust against such attacks. These concepts include transforming the object into some transform domain before embedding the mark. There are also many different ways to embed or detect a mark, strategies to choose image locations for embedding or reading it, even various ideas of what a watermark should consist of or how it should be organized before embedding it into an image. However, though StirMark is well-known and freely available, only few watermarking schemes proposed since then have claimed robustness against it which is a good indication that the current state of the art in image copyright marking is still far from having reached an acceptable level of robustness against attacks. To make things even worse, the robustness requirement often contradicts the requirement of maintaining an acceptable image quality after marking, so that often some watermark robustness has to be sacrificed to achieve a reasonable compromise between both these requirements.

E. Blind and Public Watermarking

Secondly there is the important question of whether or not the original unmarked image may be used for watermark detection. If the original image is present, it becomes much easier to undo certain attacks to the marked image, and the detection result will most likely be more reliable. Such watermarking schemes are called non-blind or public watermarking, while schemes that do not use the original image are referred to as blind. Despite of its obvious technical benefits, non-blind watermarking introduces problems when it comes to proving rightful ownership. Zeng et al. point out in that if the original image is used for watermark detection, the claim resulting from the detection results is actually based on the relationship of two images to each other: the original and the marked image. This can be exploited by counterfeit attacks aiming to invalidate the claim of ownership. In general, blind watermarking is considered a necessary requirement for being able to prove rightful Ownership. The watermark is used to support claims on rightful ownership of an image. It can also help to detect unauthorized copies and by embedding serial numbers to track down the licensee from who a pirate copy originated.

F. Image Adaptive Watermarking

Another aspect in the design of watermarking techniques is the fine-tuning of image degradation introduced by the watermark. Technically, every watermark degrades the cover-image, but the human eye is insensitive enough not to notice relatively minor image degradation for a fair amount of payload3. Depending on the watermarking application the marking scheme needs to consider how much and what kind of degradation is acceptable. In robust watermarking, the requirement of little image degradation often stands in obvious conflict with the requirement of robustness against image processing attacks. Therefore image adaptive watermarking uses the cover-image's properties around the embedding locations to determine the maximal intensity that can be used for embedding. There has been intensive research in this field including using models of the human visual system (HVS). The complexity of image adaptive watermarking techniques depends a lot on an image's embedding domain; creating and using visual models requires a lot of filtering and processing in the spatial domain, suffers from the partial loss of spatial support in the DCT or DFT (discrete Fourier transform) domains but is actually supported by the DWT.

G. Second Generation Watermarking

Finally, there are different ways in which watermarking schemes choose the embedding locations at marking and aim to find them back when detecting the mark. Some schemes simply mark all pixels (or coefficients), some choose and memories particular coordinates. A relatively new class of techniques is called second generation watermarking. Such schemes use the image's features rather than fixed coordinates because geometric attacks are likely to move pixels about in the image. Consequently this involves the application of feature detection techniques for both, determining features (according to whatever definition) for marking and later finding them back for detection. The research project presented in this thesis aims to find ways to improve robust and blind second generation watermarking schemes operating in the DWT domain, while maintaining image quality.

III. OBJECTIVES

This paper is concerned with robust watermarking of digital images. The main objectives are: achieve or at least come close to robustness watermarking benchmark while maintaining acceptable image quality. Existing research on robust image watermarking and image compression suggests that the Discrete wavelet transform (DWT) can provide a domain for embedding and reading watermarks with good properties for both, robust and invisible embedding and dealing with perceptual image features which are important for choosing and/or finding marking locations. A particular focus is thus put on investigating and exploiting the DWT's properties for robust image watermarking.

IV. PROPOSED ALGORITHM

A. Watermark Embedding

1. Select an Image
2. Detect skin Pixels & Recognize Face
3. Crop Face.
4. Segments image into compressed & rarefaction regions wlet (wavelet segmentation).
5. Select rarefaction regions.
6. Select watermark Image
7. Set Watermark Image Pixels into rarefaction regions by preserving content of an input image.
8. Save Result Watermarked image.
9. Stop

B. Watermark Extraction

1. Input Watermarked Image
2. Segments image into compressed & rarefaction regions (wavelet segmentation).
3. Select rarefaction regions.
4. Extract watermarked pixels bits from rarefaction regions.
5. Generate an Image from extracted bits.
6. Save Result.
7. Stop

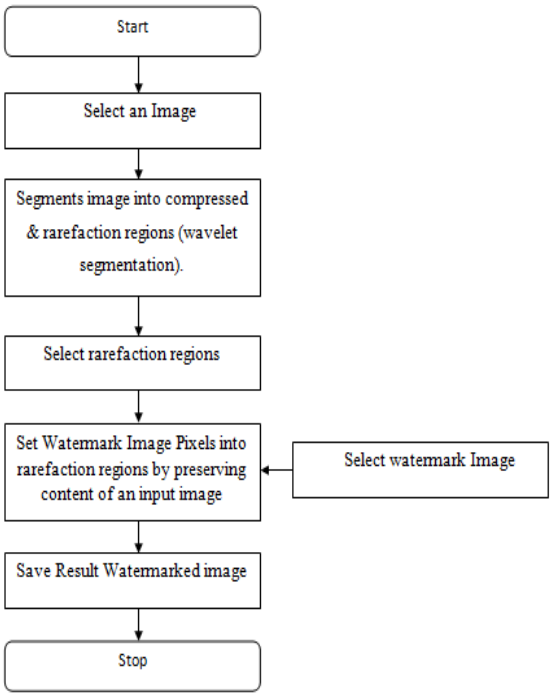

Fig. (2) Watermark Embedding

C. Face Detection with skin Color

The majority of existing methods have in common the de-correlation of luminance from the considered color channels. Luminance is underestimated since it is seen as the least contributing color component to skin color detection. Here we use a new color space which contains error signals derived from differentiating the grayscale map and the non-red encoded grayscale version.

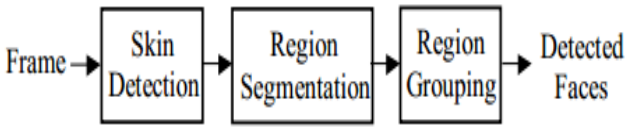

Fig.(4)

The advantages of the approach are the reduction of space dimensionality from 3D, RGB, to 1D space advocating its unfussiness and the construction of a rapid classifier necessary for real time applications.

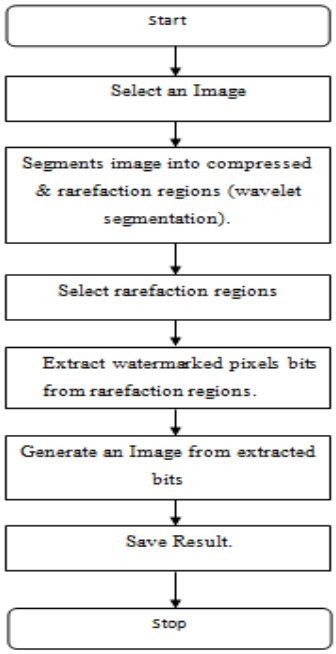

Fig. (3) Watermark Extraction

The proposed method shown in fig. (4) generates a 1D space map without prior knowledge of the host image.

```
R > 95 AND G > 40 AND B > 20 AND
max{R, G, B} – min{R, G, B} >15 AND
|R – G| > 15 AND
R > G AND R > B
OR
R > 220 AND G > 210 AND B > 170 AND
|R – G| <= 15 AND
R > B AND G > B
```

D. Features Detection

To locate the face region, we first identify the hair region that appears darker. Then the face region can be determined by growing the region with the similar color sampled below the hair region. The original image is then converted to a binary image where pixels with color values larger than a pre-defined threshold are set to 1, and other pixels are set to 0. On this binary image, pixels with value 1 are accumulated both

horizontally and vertically. Then the following rules are applied to locate feature points.


1. Because of the symmetry of a human face, the central peak of the vertical projection represents the line passing through the nose and the mouth.
2. After finding the nose-mouth line, the left and right peaks are located to find the left and right eyes, respectively.
3. From the horizontal projection, if the first peak occurs at the beginning of face region, it is the hair region's bottom line, so that next peak would be the brow line. Otherwise, the first peak represents the brow line, the next peak is the eye line, and the next 2 is the nose line.
4. The cross sections of the vertical and the horizontal projection are therefore the feature points. Positions of the feature points are further refined. For examples, at the location of left eye we search for then left most corner.

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method:

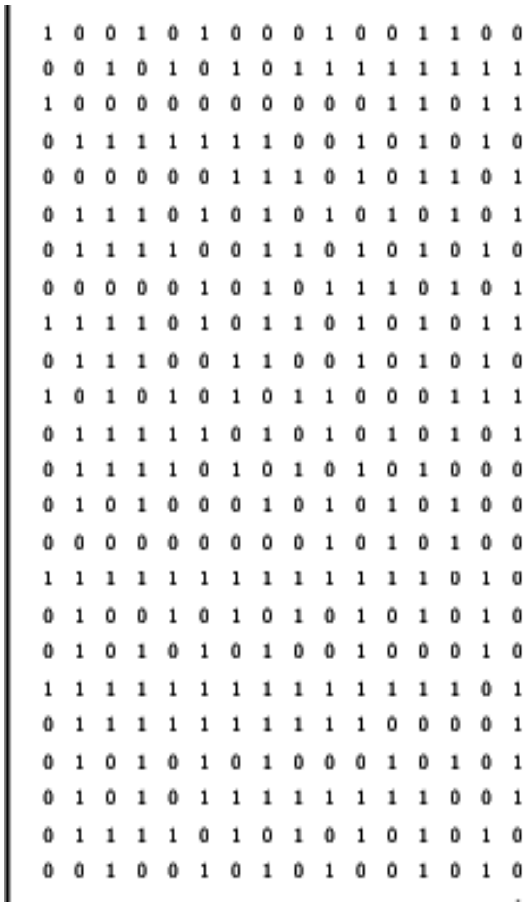

Fig. (5) Original Image Pixels

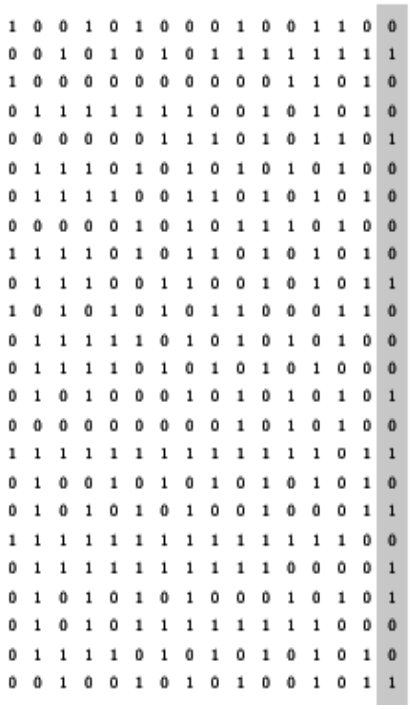

Fig. (6) Watermarked Image Pixels

In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo.

The main advantage of the LSB coding method is low computational complexity of the algorithm while its major disadvantage : As the number of used LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased. Low Bit Encoding is therefore an undesirable method, mainly due to its failure to meet the Steganography requirement of being undetectable.

V. EXPERIMENT RESULT

Tables show the Experimental Results

Table (i)

LSB Method	*Discriminates Value*
Country	**60**
Violin	**56**
Pop	**65**
Quantization error	
Method	***Error***
LSB	**-1 to + 1**
3rd LSB	**-8 to + 8**
4th LSB	**-16 to + 16**
5th LSB	**-32 to + 32**
6th LSB	**-64 to +64**

Quantization error by Proposed Method is +/- 1.

Table (ii)

Method	Data Hiding Capacity	Data Extraction	Flipping Required
LSB	One bit/Sample	100%	No
3rd LSB	One bit/Sample	100%	Yes
4th LSB	One bit/Sample	100%	Yes
5th LSB	One bit/Sample	100%	Yes
6th LSB	One bit/Sample	100%	Yes
Proposed Method	One bit/Sample	50-60 %	No

Table (iii)

Hiding method/music	Country	Violin	Pop
Discrimination values (%)			
Standard algorithm (3 LSBs)	52	53	48
Standard algorithm (4 LSBs)	55	70	67
New algorithm (3 LSBs)	51	48	49
New algorithm (4 LSBs)	53	46	53
Mean opinion score (MOS)			
Standard algorithm (3 LSBs)	5.0	4.9	5.0
Standard algorithm (4 LSBs)	4.2	3.5	4.0
New algorithm (3 LSBs)	5.0	5.0	5.0
New algorithm (4 LSBs)	5.0	4.8	5.0

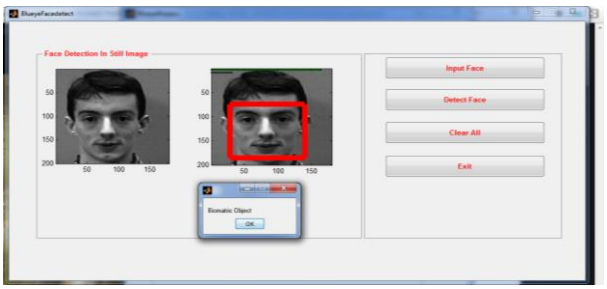

Fig. (7) Input Image with Face detected(Biometric Pass)

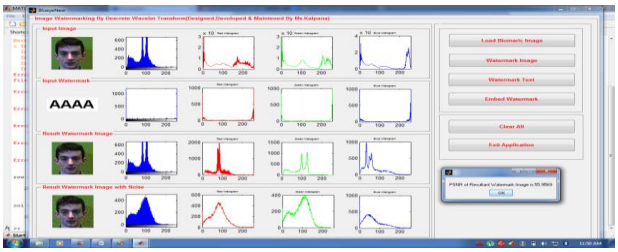

Fig. (8) Watermark Embedding

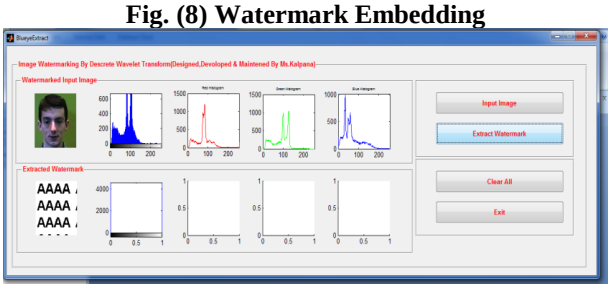

Fig. (9) Recovered Watermark Image

VI. CONCLUSION

The key idea of the algorithm is watermark bit embedding that causes minimal embedding distortion of the host image. Visual tests showed that described algorithm succeeds in increasing the depth of the embedding layer from 4th to 6th LSB layer without affecting the perceptual transparency of the watermarked image signal. The improvement in robustness in presence of additive noise is obvious, as the proposed algorithm obtains significantly lower bit error rates than the standard algorithm. The steganalysis of the proposed algorithm is more challenging as well, because there is a significant cryptography provided for data security.

REFERENCES

1. Ahmed Ch. Shakir," Steno Encrypted Message in Any Language for Network Communication Using Quadratic Method", in Journal of Computer Science 6 (3), Science Publications, 2010, pp. 320-322 .
2. Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas,"Data Hiding in Video", in International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.
3. Andreas Westfeld and Gritta Wolf," Steganography in a Video Conferencing System", Information Hiding 1998, Springer-Verlag Berlin Heidelberg 1998 pp. 32-47.
4. D. P. Gaikwad and Dr. S.J. Wagh, "Color Image Restoration for Effective Steganography", in i-manager's, Journal on Software Engineering, Vol. 4 l, No. 3 l , January - March 2010, pp.65-71.
5. D.P.Gaikwad and Dr. S.J.Wagh, "Image Restoration Based LSB Steganography for Color Image", AISA-PACIFIC Regional Conference in ICTM-2010 on Innovations and Technology Management at Mumbai
6. Richard E. Woods & Rafael C. Gonzalez , Digital Image Processing (second edition), Pearson Prentice Hall.
7. Neil F. Johnson and Sushil Jajodia,"Exploring Steganography: Seeing the Unseen", George Mason University.
8. S. Suma Christal Mary, "Improved Protection In Video Steganopgraphy Used Compressed Video Bitstream ," in International Journal on Computer Science and Engineering ,Vol. 02, No. 03, 2010, pp.764-766.
9. Saurabh Singh and Gaurav Agarwal,"Hiding image to video: A new approach of LSB replacement", in International Journal of Engineering Science and Technology Vol. 2(12), 2010, pp.6999-7003.
10. Steganography on new generation of mobile phones with image and video processing abilities, as appeared Computational Cybernetics and Technical Informatics (ICCCCONTI), 2010 International Joint Conference on 27-29 May 2010 in Timisoara, Romania .
11. D.-C. Wu and W.-H. Tsai " A steganographic method for images by pixel-value differencing", in Pattern Recognition Letters, Vol. 24, 2003, pp.1613–1626.
12. F Hartung., B. Girod."Steganoing of uncompressed and compressed video", in Signal Processing,Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998, 66 (3), pp. 283-301.

AUTHORS PROFILE

Kalpana Bhelotkar B.E. (ET & T) in 2003, from RGPV University Bhopal, persuing M.E. (Commn.) from SSCET Bhilai, working as lecturer in CIT Rajnandgaon (C.G.) published some papers in National and International journals, Area of interest in hardware design and Watermarking.

Sandeep B. Patil B.E., M.E. Ph.D. Scholar published various papers in National and International journals and conferences, working as Asso. Professor in SSCET Bhilai, guided numbers of students of B.E. and M.E., Area of interest Watermarking, Steganography, Matlab coding, Microwave communication, and Radar Engineering.