Design and Analysis of Hybrid Model using DELPHI Encoding for Visible and Invisible Image Watermarking

Swati Dhiman
EEE dept.
Arni University
Kathgarh (H.P), India

Onkar Singh
ECE dept.
Arni University
Kathgarh (H.P), India

ABSTRACT
As the digital data is transferred over the internet which may harm the digital data like tampering of data etc. Therefore, the need of digital data protection has been increased with the advancement in the technology. Watermarking is a technique used to protect the digital data. Digital watermarking is a technique by using which user can get the copyright of its product which prevents the data from tampering. Many techniques are available for video watermarking like Discrete Wavelet Transform, Least Significant Bit Technique etc. [2].The properties of digital watermarking are For copy control, In fingerprinting, For identification of ownership, For Authentication, Monitoring of digital video broadcast, In video tagging etc. [1].

Keywords
DCT, DFT, DWT, LSB, Watermarking, Security.

1. INTRODUCTION
Digital watermarking is a technique which is used to hide the digital data behind a data. Digital watermarking is a type of steganography. Digital watermarking follows the steganography and hide the digital data behind other data but in this source image and hidden image both has the highest preference. The concept of digital watermarking comes from the concept of image watermarking where the copyright identification is appended on the host image for the purpose of security of image [2].

Fig. 1 Example of image watermarking

Once a watermark is embedded on digital data it can be removed anytime according to the need. The process of image watermarking is different from image watermarking. The process of Digital watermarking has two main principles:

1. Embedding process
2. Extraction Process

Embedding Process

This contains the selection of watermark which is going to embed on the digital data. The selection of watermark depends upon the kind of data it is, whether it is original data or compressed data and whether the watermark is visible or not [3].

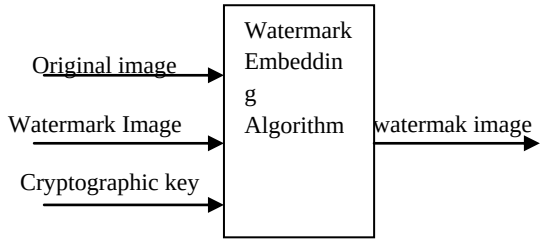

Fig. 2 watermarking embedding process

Extraction Process

In this process to demonstrate or show the concern of copyright on the data and to make sure that the purpose of watermarking has been achieved the watermark is extracted from the watermarked digital data. The extracted watermark may vary from the original watermark [3].

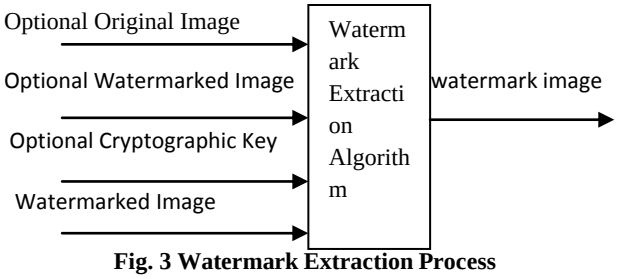

Fig. 3 Watermark Extraction Process

Digital Watermarking has a large area of application where it is used like:

- Copyright protection
- Source tracking (different recipients get differently watermarked content)
- Broadcast monitoring (television news often contains watermarked video from international agencies)
- Video authentication.

2. TECHNIQUES FOR FACE RECOGNITION

Digital watermarking can be done by using algorithms. These techniques are based on certain criteria [4].

2.1 According to Document:

1. Image Watermarking: It is the Process of data hiding behind an image
2. Video Watermarking: This is the process of adding watermark to a video to prove the concern of owner.
3. Audio Watermarking: The process of hiding data behind audio data.
4. Text watermarking: The process of adding watermark to the documents in order to prevent them for being copied by others.

2.2 According to Working Domain:

2.2.1 Spatial Domain:

This is the process of adding watermark to the data. It modifies the pixels of randomly selected data. In this the raw data is directly loaded to image pixels. It uses LSB (Least Significant Bit) algorithm and Patchwork technique.

Least Significant Bit Algorithm: This algorithm is easy to implement and understand. It adds the watermark to the lowest order bit of each pixel of the image. As the watermark is embedded at the lowest bit of the pixel similarly the extraction is done by detecting the lowest bit of the pixel in the image and then the watermark is extracted from the data.

Patchwork Technique: Patchwork technique is based on some statistical result because it embeds the watermark in the data with a specific statistics by using Gaussian distribution. The extraction of watermark can be done by combining the received signals with expected form.

2.2.2 Frequency Domain:

It is also known as Transform domain. It uses several frequencies to

1. Insert the watermark in the data. It uses domain methods to implement the watermark as:

DCT (Discrete Cosine Transformation): It adds watermarks to a still digital image. In this the image is presented in the form of frequencies of cosine. Then 8*8 blocks of the image is considered to calculate the DCT of the image.

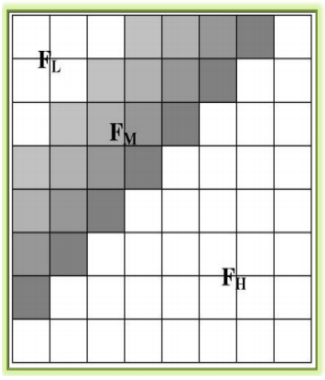

Fig.4 frequency bands generated in DCT

DWT (Discrete Wavelet Transform): It generates a time frequency of particular signals at a given time. It converts the image into three dimensions horizontal, vertical, diagonal respectively. The transformations are base4d on small waves namely wavelet.

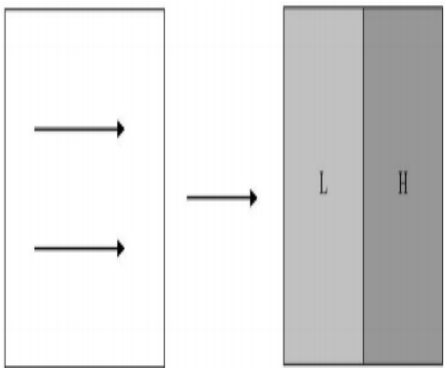

Fig. 5 Horizontal Transformation

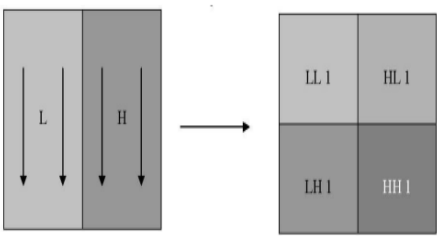

Fig. 6 Vertical Transformation

DFT (Discrete Fourier Transform): It converts the unique functions into frequency components. In case of digital image, the even functions are considered as the frequency of sine or cosine and multiplied with the weighing function. It generates the coefficient of Fourier transform in the signal.

2.3 According to Human Perception:

2.3.1 Visible watermarking:

In this technique the embedded watermark is visible to the end user. It is the earlier technique of watermarking. The watermark is embedded on the cover page of the image.

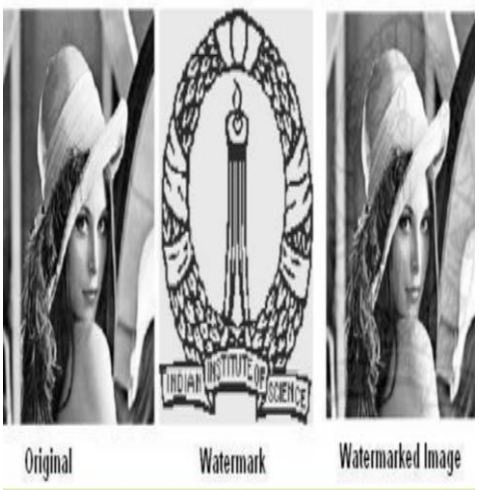

Fig. 7 Visible Watermark

2.3.2 Invisible Watermarking:

Invisible Watermarking is that kind of watermarking technique in which embedded watermark is not visible to the viewer.

2.3.3Dual watermarking:

It is a combination of both visible and invisible watermarking technique embedded on the cover page of the image.[5]

3. PROBLEM FORMULATION

Watermarking is a technique of hiding digital data in the image for authentication purposes. Watermark that is to be embedded in the image can be visible or invisible depending on the type of technique used to embed the watermark. The watermark embedded should not change the information of the image. In old approaches fractal encoding was used for watermarking an image. The disadvantages of using fractal encoding for watermarking were high cost, less security and data compression. A challenging problem of ongoing research in fractal image representation is how to choose the $f1,...,fN$ such that its fixed point approximates the input image, and how to do this efficiently. The fractal encoding in image watermarking was used for image transformation into compressed form and the watermark pattern was embedded into the image. This was cumbersome as the image having large number of pixels find it harder to embed the data and the data compression took place. The security of the watermarked image with fractal encoding was lower as the data could be encrypted by any unauthorized user also. So a new technique needs to be designed that can efficient embed watermark in the image and the drawbacks of this technique are also overcome using the new proposed technique.

4. PROPOSED WORK

While these are all security devices for digital material and the terms are frequently used interchangeably, they are nevertheless three distinctly different protection methods. Encryption works by locking an object file with a 'key' and providing that key only to authorized users. Whilst this generally provides a high degree of active security, once an encrypted file is opened, the contents become unprotected and may then be readily edited, copied and disseminated without any further form of control. Visible watermarking usually places a visible mark superimposed onto an image. These watermarks can be removed by image processing software and, for this reason, do not offer any high degree of protection. Invisible watermarking, sometimes known as fingerprinting or digital Steganography, protects image data at a very deep level. In this we will develop a system in which firstly user will as what type of watermarking does it need. After this two algorithm for visible and invisible each will be implemented and we will compare results of both techniques can also be named as hybrid system for watermarking in visible and invisible watermarking. The technique which will be used for the visible watermarking can be Spatial domain based watermarking and for invisible one the technique can be recent and updated with the traditional ones that can be use of DELPHI approach in LSB based watermarking which is advanced and security oriented technique

5. METHODOLOGY

The methodology of the proposed work is defined below. This proposed method is considered to be better and efficient than the traditional method:

1) Initially an image is selected from the data set of the images, in which the data is to be embedded and is send to the receiver at the other end.
2) After the selection of the image form the given set, next step is to choose the type of watermark that is to be inserted in the image.
3) Firstly the visible watermark is selected; Next step is to perform the watermarking process .This visible watermark is added in the selected image.
4) Finally the watermarked image is obtained and the calculation of the results is done.
5) Now the invisible watermark is selected, this invisible watermark is added into the image that is browsed earlier form the given data set of the image.
6) Now apply the DELPHI Coding approach the selected watermarked image for the compression of the image, after this the LSB encryption algorithm is applied on the image on which earlier the coding is applied .Finally watermarked obtain.

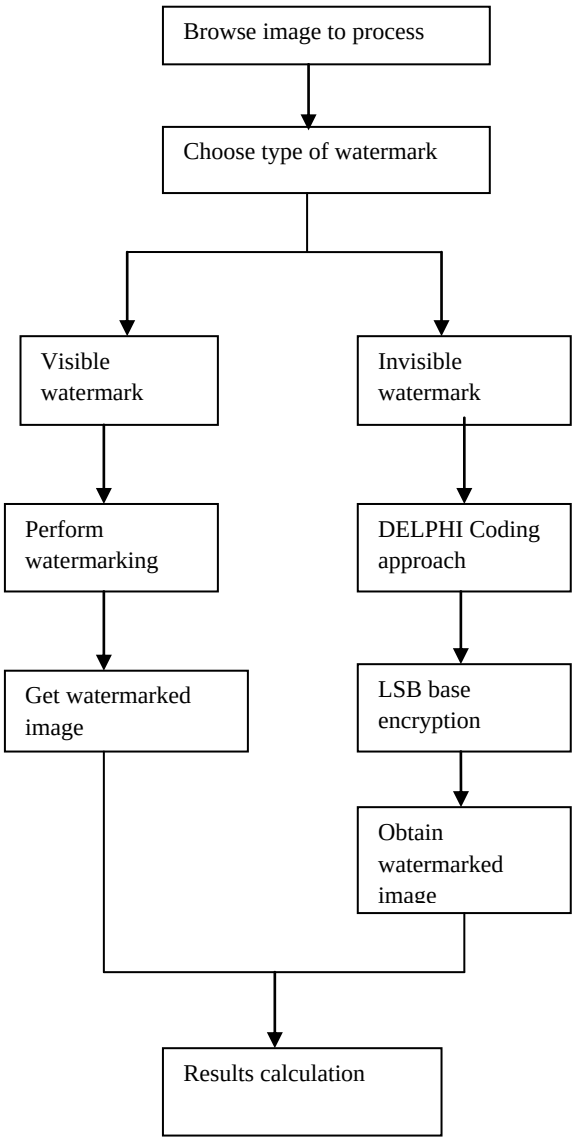

Fig. 8 Block diagram of proposed Technique

6. RESULTS ANS ANALYSIS

In this section of the paper, results have obtained after applying encryption or watermarking to the original image. It also includes the comparison that has been performed on the proposed method with the existing method.

(a)Original image

(b) Watermark

(c) Visible watermark

(d) Invisible watermark

In above figure (A) shows the original cover image, on which we are going to embed the watermark.

In figure (B) image of the watermark is shown which will be used as watermark.

In figure (C), shows the image with visible watermark.

In figure (D), shows the image with invisible watermark

Fig 9 shows the comparison between old techniques and proposed techniques with respect to the Peak signal to noise Ratio. From figure 9 it is clear that the Peak signal to noise ratio is higher after applying the proposed technique whereas noise ratio is low in old work.

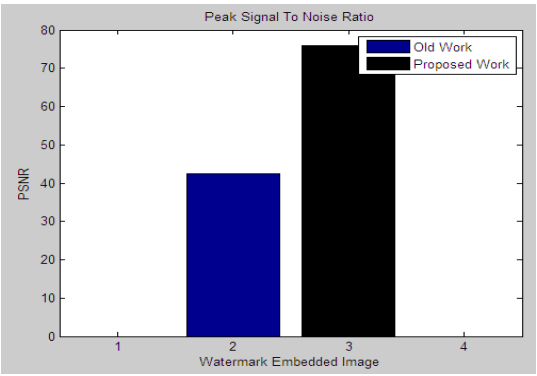

Fig 9.Comparison of traditional and propose technique

Traditional FND:-0.26 ---- Proposed FND:--0.03

Traditional FPD:-0 ---- Proposed FPD:-0

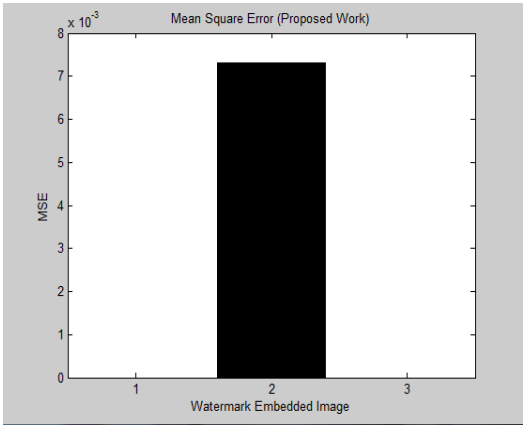

Fig. 10 MSE

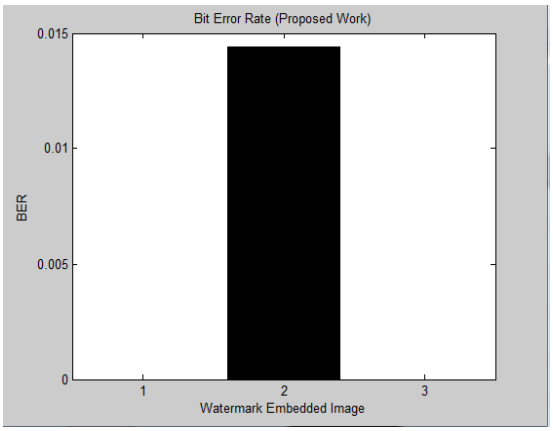

Fig. 11 BER

Table 1. Performance Value of Different Technique

Method	Traditional	Proposed
PSNR	40	70
FND	0.26	0.03
FPD	0	0

7. CONCLUSION

Image watermarking is a process of hiding the data into the image. Watermark that is to be embedded in the image can be visible or invisible depending on the type of technique used to embed the watermark. The watermark embedded should not change the information of the image It is observed after implementing the traditional methods of image watermarking they are not that much efficient in case of security issues, so in proposed work an approach of data compression algorithm for increasing the security of the data . Firstly the format of the image is changed and then by using the compression algorithm the data is compressed first and then it is send to the receiver.

From the results obtained it is concluded that this proposed method is efficient than the traditional methods as the security of the data is increased. By increasing the security of the data the efficiency of the system is increased

8. REFERENCES

[1] Antonio Cedillo-Hernandez," Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT", ELSEVIER, Vol 97, Pp 40-54, 2014

[2] Mahima Jacob, Saurabh Mitra," Video Watermarking Techniques", IJRTE, Vol 4, Pp 1-4,2015.

[3] Lalit Kumar Saini, Vishal Shrivastava," A Survey of Digital Watermarking Techniques and its Applications", IJCST, Vol 2, Pp 70-73,2014

[4] Rakesh Ahuja, S. S. Bedi," All Aspects of Digital Video Watermarking Under an Umbrella", Ijigsp, Vol 12, Pp 54-73, 2015

[5] Monika Patel,Priti Srinivas Sajja," Analysis and Survey of Digital Watermarking Techniques", ijarcsse, Vol 3, Pp 203-210, 2013

[6] Chandra, M.(2010), "Digital watermarking technique for protecting digital images" Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference , Volume:7, Pp 226 – 233,

[7] Vinita Gupta M(2014), "A Review on Image Watermarking and Its Techniques" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1,Pp 92- 97

[8] Manjit Thapa (2011)" Digital Image Watermarking Technique Based on Different Attacks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4,Pp 14 -19

[9] Radhika v(2013), "Comparative Analysis of Watermarking in Digital Images Using DCT & DWT" International Journal of Scientific and Research Publications, Volume 3, Issue 2,Pp 1-4

[10] Zhu Yuefeng (2015), "Digital image watermarking algorithms based on dual transform domain and self-recovery" international journal on smart sensing and intelligent systems vol. 8, no. 1,pp 199- 219

[11] Puneet Kr Sharma(2012), "Analysis of image watermarking using least significant bit algorithm "International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4,Pp 95 -101

[12] Md. Selim Reza(2012), "An Approach of Digital Image Copyright Protection by Using Watermarking Technology" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2,Pp 280 -286

[13] Shrusti Porwal(2013), "Data Compression Methodologies for Lossless Data and Comparison between Algorithms" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2,Pp 142- 147

[14] Debashis Chakraborty, "Efficient Lossless Color Image Compression Using Run Length Encoding and Special Character Replacement"

[15] M. Baritha Begum, December 2013, "A New Compression Scheme for Secure Transmission" International Journal of Automation and Computing 10(6), Pp 578-586

[16] Amrita Jyoti, February 2014, "An Advanced Comparison Approach with RLE for Image Compression" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2,Pp 95- 99

[17] M.VidyaSagar,(2013) , "Modified Run Length Encoding Scheme for High Data Compression Rate" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 12,Pp 3238-3242[18] P. M.Sandeep, March 2013, "FPGA Bit-stream Compression Using Run-length Encoding"

[18] J. Anitha(2010), "A Color Image Digital Watermarking Scheme Based on SOFM "IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5,Pp 302-309

[19] Jobenjit Singh Chahal (2013)" A Review on Digital Image Watermarking "International Journal of Emerging Technology and Advanced Engineering Website Journal, Volume 3, Issue 12,Pp 482 -484

[20] Neil F. Johnson , "An Introduction to Watermark Recovery from Images "

[21] Amir Houmansadr , "A Digital Image Watermarking Scheme Based on Visual Cryptography "

.