Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Semi Fragile Watermarking Scheme

Pooja Gupta[1], Neha[2]
[1,2] Department of Computer Science, Jamia Hamdard

Abstract- In Watermarking techniques, the information that is conveying the watermark is embedded in an object, which can be an image, audio or video. Watermarking can be fragile or non-fragile depending upon user's necessities. The fundamental concern of advanced watermarking is to demonstrate possession and to provide additional assurance of the implanted data. This paper gives brief outline of existing watermarking systems and their requirements. Semi fragile watermarking is implemented here using MATLAB on image object.

Keywords— Information hiding techniques, Watermarking, Semi fragile, Benign Transformation, Embedding process, Extraction Process

I. INTRODUCTION

In electronic data security, watermarking plays a vital role as it is an initiative for the copyright ownership protection. As the growth and development of internet has made digital data widely available and accessible, it has become highly challenging to protect this data from piracy [5].Watermarking is one of the emerging technologies in which data is visible but cannot be duplicated and protects original owner ship of a redistributed copy. Watermarking allows the user to embed some special pattern or data into digital content without changing its perceptual quality. It is one of the major information hiding techniques. The purpose of watermarking includes copyright protection, fingerprinting, copy protection, broadcasting monitoring and data authentication. The digital image watermarking is inalterably embedded into the image/data and should not degrade the quality of the data. Information hiding techniques are classified as shown below:

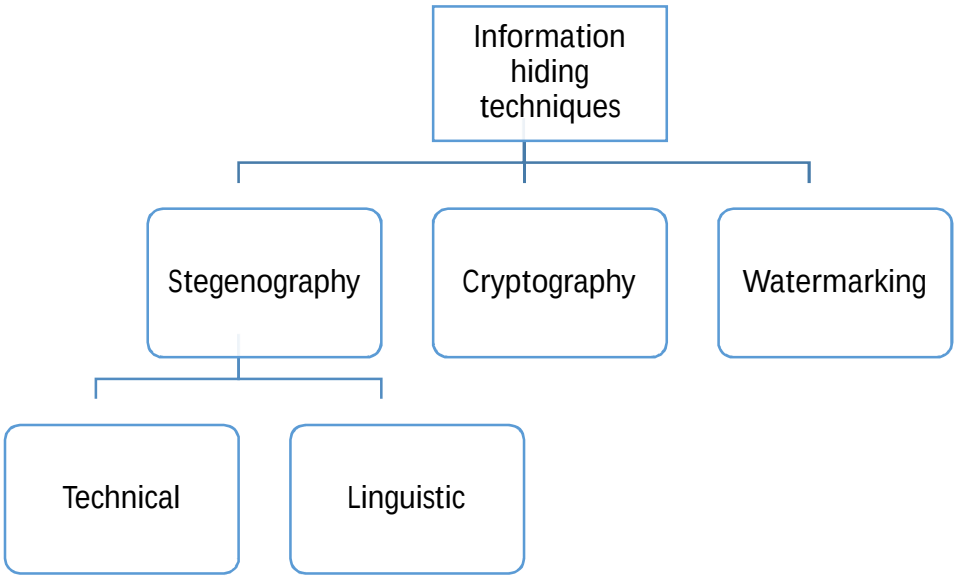

Fig 1 Classification of Information Hiding Techniques.

Steganography means concealing one piece of information within another. In this technique, the message is hidden in such a manner that no one apart from the sender and the intended receiver, suspects the existence of the message, a form of security through obscurity. Cryptography is most often associated with scrambling plaintext into cipher text (a process called encryption), then back again (known as decryption). A watermark is a form, image or text that is impressed onto paper, which provides the evidence of its authenticity. In digital watermarking case a pattern of bit is inserted into the digital information which identifies the files of copyright. A generic watermarking system is represented in fig 3. It can further be classified according to human perception, robustness, and document.

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

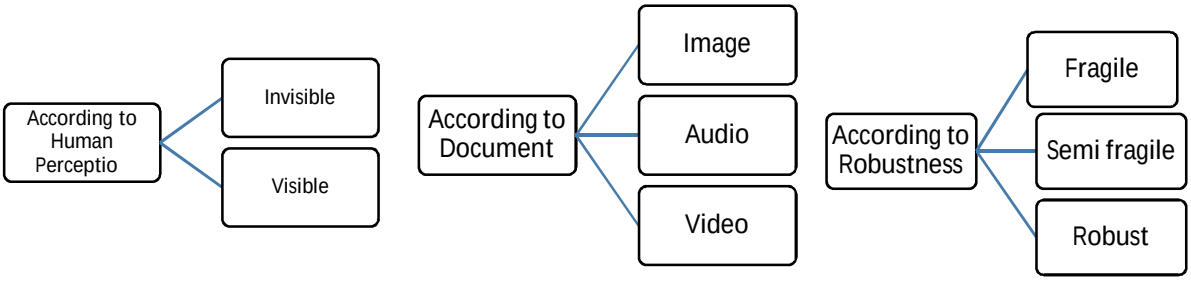

Fig 2 Classification of watermarking.

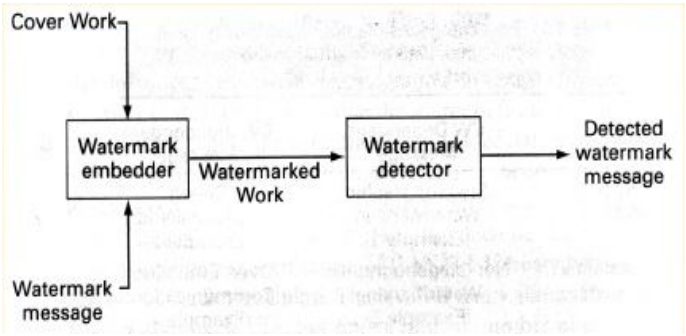

Fig 3 A Generic watermarking system.

II. ESSENTIALS OF WATERMARKING

Some important design features need to be taken into consideration while developing an optimal image watermarking system, which are listed below:

A. Robustness

bustness [9] is one of the major design issues for all watermarking applications. A watermark is called robust if it resists a designated class of transformation. The watermark should be robust against various signal processing attacks like digital-to analog & analog-to-digital conversions, filtering, compression, and geometric transformation [10] of host image.

B. Perceptual Transparency

Another requirement of watermarking is perceptual transparency [8]. The watermark which has been embedded with the owner's information should not degrade the quality of the actual signal. The watermark is not visible to the human eye. It can only be detected by special processing or dedicated algorithms.

C. Security

One of the desirable qualities of watermarking is that it must be strongly resistant to the piracy of the information by any unauthorized agent. The security of the watermarking framework is subject to the utilization of private or mystery key.

D. Verification and reliability

The Watermark ought to have the capacity to give complete and reliable data to demonstrate its' responsibility for the security of items. The watermarking strategy ought to be giving the unwavering quality of recuperation of watermark. The vigour of the watermarking strategy is reliant upon how safely and shrewdly the watermark is installed into the host motion with no observable change. Robustness of the algorithm to attack and the quality of the watermarked image are related properties that are indispensable. All applications presupposing security and used in the checking of the watermarking frameworks require this sort of stamping so as to survive any sort of adjustment or deliberate expulsion presented by standard or malignant handling and attack.[4,12]

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III. SEMI-FRAGILE WATERMARKING

Watermarking is the procedure that installs watermark into an image with the end goal that the watermark will be identified and additionally extricated later to make a statement about the image. The technique consists of two main sub processes namely:

1) Embedding process:

In embedding process, the original host signal and the secret key as the inputs, create the watermark signal [1]. The block diagram of embedding process [4,19] is shown in fig. 4:

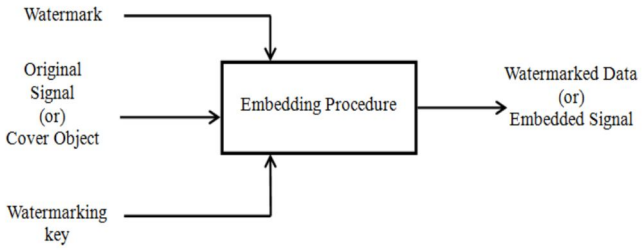

Fig 4 Watermarking embedding process

2) Extraction Process: The watermarking technique in which the original data is not available to the watermark extraction system is popularly known as Blind detection whereas the technique in which the original data is available to the watermark extraction system is called Non-Blind Detection. Fig.5 illustrates typical watermarking extraction process [1,19].

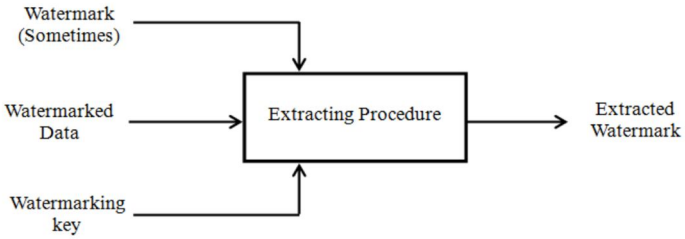

Fig 5 Watermarking extraction process

IV. SEMI FRAGILE WATERMARKING TECHNIQUE

If a watermarking technique resists benign transformation but fails detection after malignant transformation then it is known as Semi fragile Watermarking. The algorithm followed is a novel semi-fragile watermarking scheme for image authentication and tamper detection by using two complementary watermarks namely Edge-based watermark and Content-based watermark [2]. In this paper the proposed semi fragile watermark consists of four components as shown in fig 6

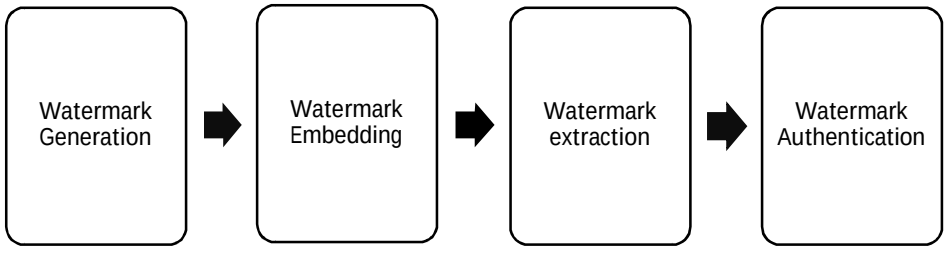

Fig. 6 Proposed Semi fragile Watermark Components

A. *Watermark Generation*

Sobel Edge detection is applied to LL3 sub-band of original image in order to obtain first (relation based) watermark i.e. Wedge. Then, logical "AND" operation is applied to LL3 sub-band of image and Wedge to get LL3p which is then quantized and further

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

used to generate Wrel (second i.e. edge based watermark)

B. Watermark Embedding

The first half of Wrel in LH1 sub-band, second half of Wrel in the HH1 sub-band and Wedge in the HL1 sub-band is embedded respectively.

C. Watermark Extraction

The same strategy is applied to extract watermark bit sequences EW1, EW2, and EW3 from LH1, HH1, and HL1 sub-bands of the Haar wavelet transform, respectively. The watermark bit sequence EW3 is reshaped to obtain the extracted content-based watermark EWedge. Watermark bit sequences EW1 and EW2 are concatenated to form the extracted watermark EWrel.

D. Watermark Authentication

The same watermark generation scheme is applied on the probe image to generate two watermarks, GWedge and GWrel.
Then, the content-based difference watermark image DiffMatrix and difference watermark sequence DiffSeq is computed for the authentication.

V. RESULTS

In Difference Matrix obtained from taking the absolute difference between EWedge (extracted content based watermark) and GWedge (generated content based watermark) –

$$u = \frac{No\ of\ Malicious\ Pixels}{No\ of\ Tampered\ Pixels} \ldots\ldots\ldots\ldots\ldots\ldots \text{eqn.(1)}$$

In DiffSeq matrix obtained from the subtraction of EWrel (extracted edge based watermark) from GWrel (generated edge based watermark) –

$$p = \frac{Total\ no\ of\ error\ bits(non-zero)}{Length\ of\ GWrel} \ldots\ldots\ldots\ldots \text{eqn.(2)}$$

Table 1. Proportion of Images With Modifications

Authenticated		Maliciously Distorted	
No. of Images	*Detected Correctly*	*No. of Images*	*Detected Correctly*
10	10	5	4

Incidentally Distorted							
Gaussian Blur		Sharpening		Gaussian Noise (μ = 0 & = 0)		Median Filtering	
No. of Images	*Detected Correctly*	*No. of Images*	*Detected Correctly*	*No. of Images*	*Detected Correctly*	*No. of Images*	*Detected Correctly*
10	10	10	10	10	10	10	10

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Table 2: Effect of compression on distortion identification

JPEG Compression	
Quality Factor	*Distortion Detected*
5	Malicious
10	Incidental
20	Incidental
30	Incidental
40	Incidental
50	Incidental
60	Incidental
70	Incidental
80	Incidental
90	Incidental

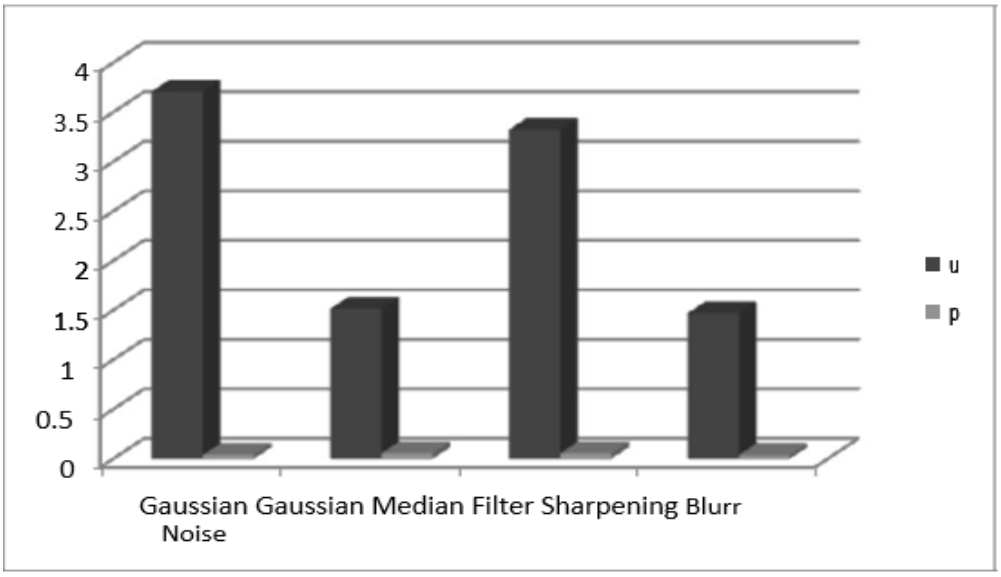

Fig 7 Comparison of image processing attacks on p's and u's

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

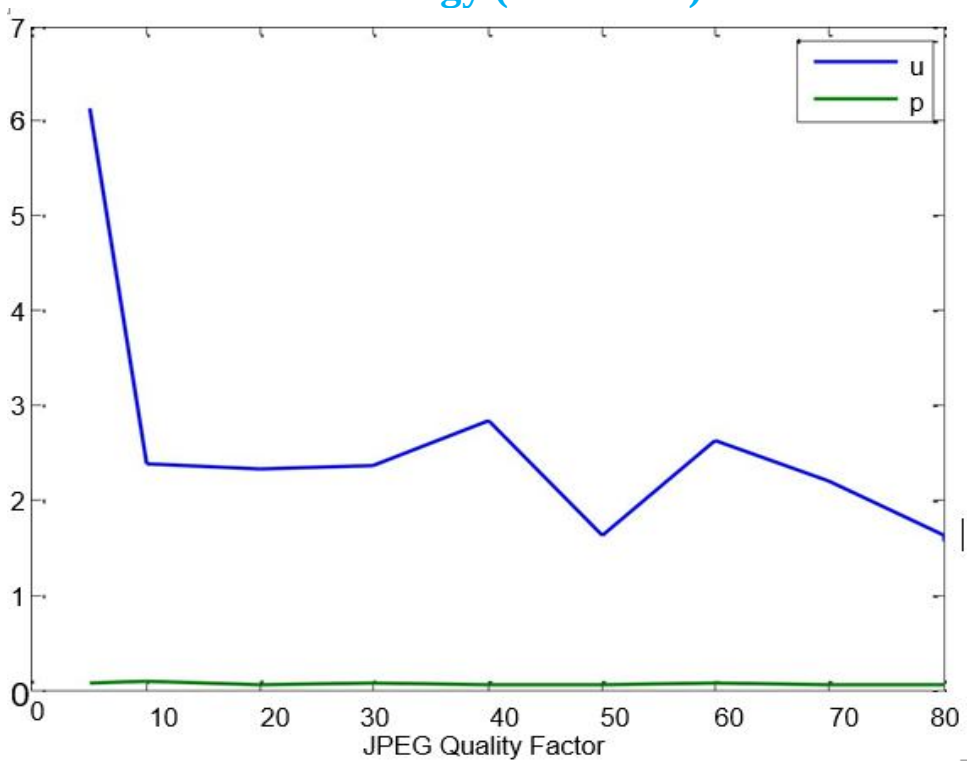

Fig 8 Comparison of JPEG compression attacks on p's and u's

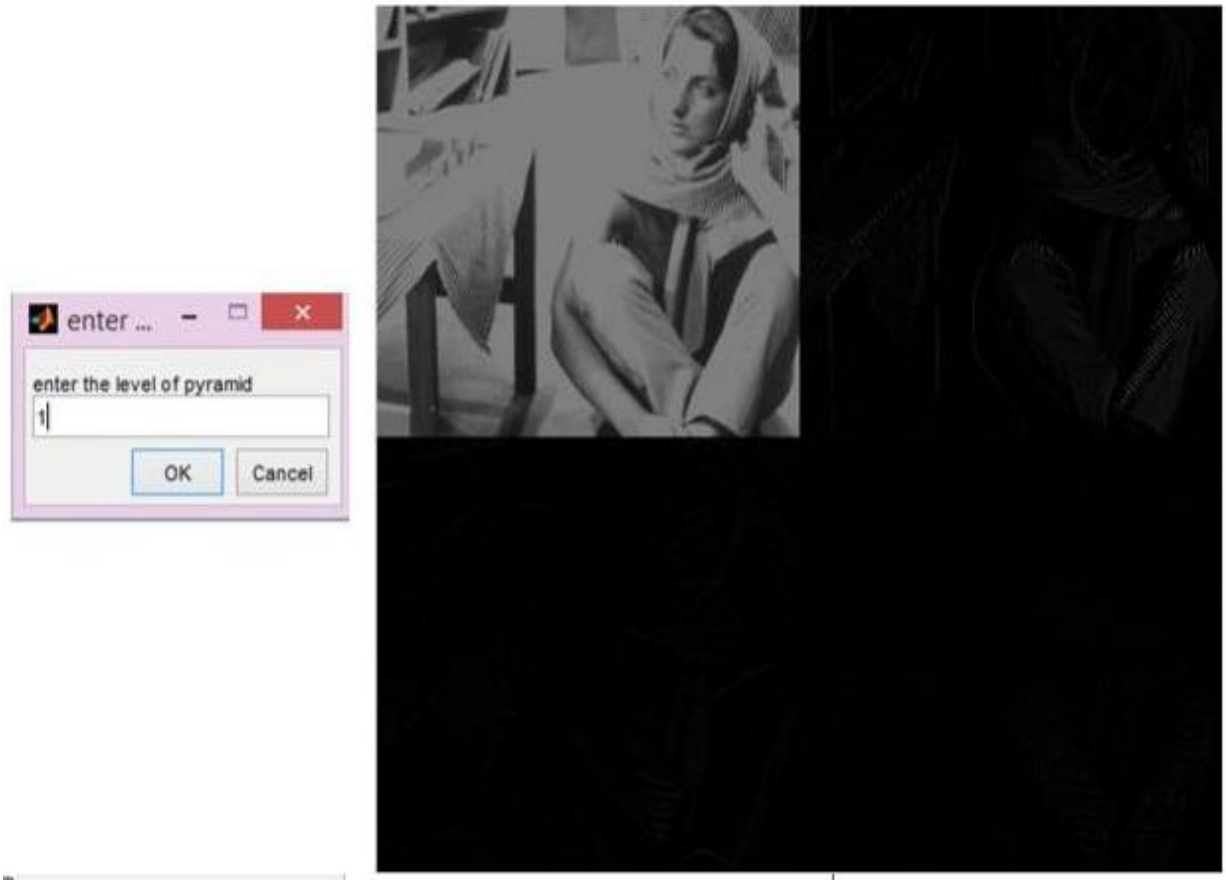

Fig 9. 1- level Haar Transformed Image

©IJRASET: All Rights are Reserved

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

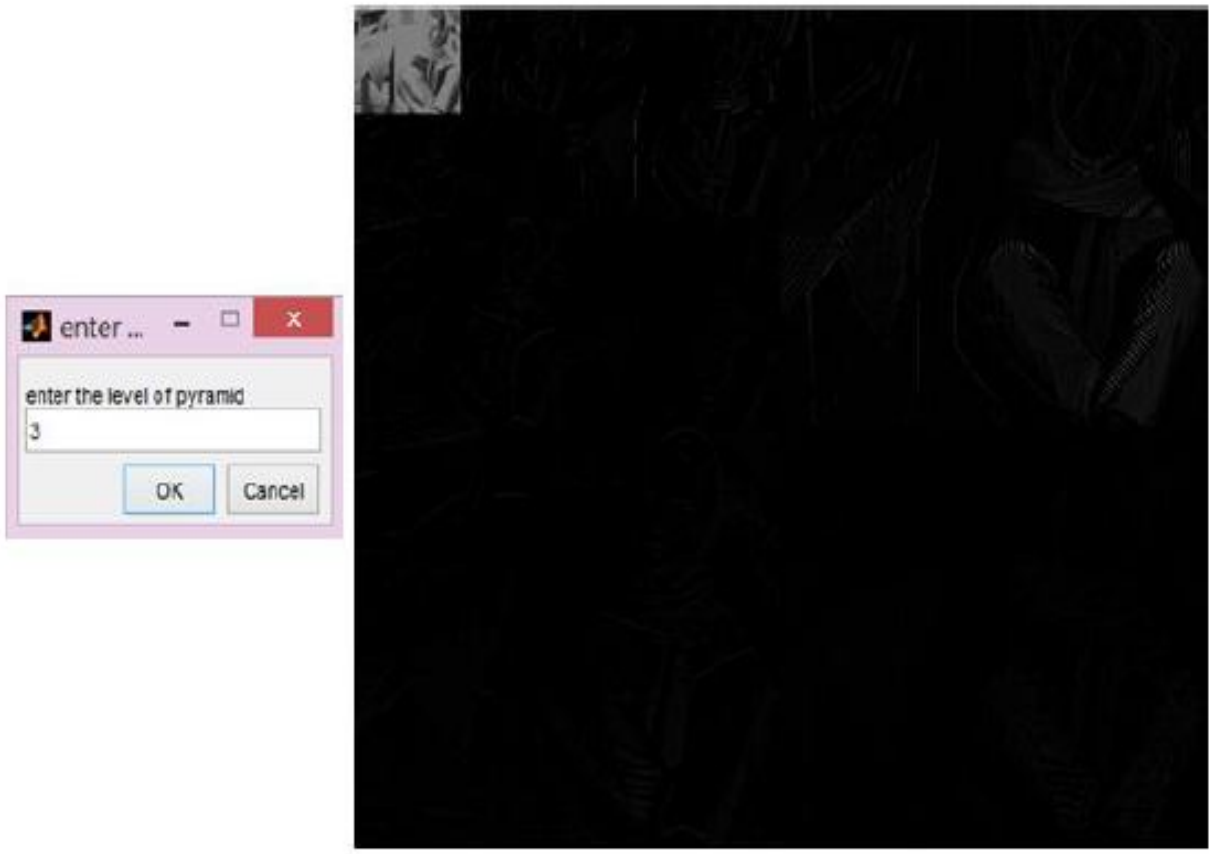

Fig 10 3-level Haar Transformed Image

Fig 11 Incidentaly Distorted image

V. CONCLUSION

There are many watermarking techniques and each one of them has different features and different capabilities. An overview of the semi fragile techniques has been done in this paper. The scheme propounded herein brings about two corresponding watermarks. An edge-based watermark sequence, which ciphers the invariant relationship between quantized wavelet coefficients, is applied to recognise any transmutation after manipulations. A content-based watermark is utilized to pinpoint the vandalized regions. The discussed scheme victoriously determines malicious attacks and the non-malicious tampering of image content.

©IJRASET: All Rights are Reserved

REFERENCES

[1] M.NavneetKumar, "WatermarkingUsingDecimalSequences,"M.S.thesis, Louisiana State University, Baton Rouge, LA, USA, 2004.
[2] Xiaojun Qi, Xing Xin, and Ran Chang, "Image Authentication and Tamper Detection Using Two Complementary Watermarks"
[3] Proakis, J.G., "Digital Communications", 3rd edition, McGraw-Hill, New York, NY1995.
[4] I. Cox,, M. Miller, et al. "Digital watermarking and steganography", Morgan Kaufmann, 2008.
[5] W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3–4) (1996) 313–336.
[6] Yang, Z. Dual Domain Semi-fragile Watermarking for Image Authentication, Master thesis, University of Toronto, Canada 2003.
[7] R. Wolfgang, E. J. Delp, "A watermark for digital images", Proc. IEEE Int. Conf. Image Processing, vol. 3, pp. 219-222, 1996
[8] P.W. Wong, N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification, IEEE Trans. Image Process. 10 (10) (2001) 1593–1601.
[9] T.H. Chen, D.S. Tsai, Owner–customer right protection mechanism using a watermarking scheme and a watermarking protocol, Pattern Recognition 39 (8) (2006) 1530–1541.
[10] C.Y. Lin, S.F. Chang, A robust image authentication method distinguishing JPEG compression from malicious manipulation, IEEE Trans. Circ. Syst. Video Technol. 11 (2) (2001) 153–168.
[11] J. J. Eggers, B. Girod, "Blind watermarking applied to image authentication", Proc. ICASSP'2001 Int. Conf. Acoustics Speech and Signal Processing, 2001-May-7
[12] P. Loo, N. Kingsbury, Watermark detection based on the properties of error control codes, IEE Proc. Vis. Image Signal Process. 150 (2) (2003) pp 115–121.
[13] Azizah, A. M., Akram, M. Z., Sayuthi, J.,Watermarking of Digital Images: An Overview,2nd National Conference on Computer Graphics & Multimedia. Malaysia. 2004.
[14] Isinkaye F. O. and Aroge T. K. "Watermarking Techniques for Protecting Intellectual Properties in a Digital Environment" JCS&T Vol. 12 No. 1, April 2012
[15] J. Lacy, R. Quackenbush, A. Reibman , D. Shur and J. Snyder, On "Combining Watermarking with Perceptual Coding". ICASSP Seattle, Washington. MMSP1.9, 1998.
[16] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," in Proc. SPIE, vol. 2420, San Jose, CA, Feb. 1995, p. 40.
[17] Pitas,I., "A Method for Watermark Casting on Digital Images", IEEE circuits and system for video technology, 1998, pp. 775-780.
[18] Hsu C. T. and Wu, J. L. Hidden Digital Watermarks in Images. IEEE Trans. on ImageProcessing, vol. 8, no. 1, pp. 55-68. 1999.
[19] Chauhan Usha, Singh Rajeev Kumar," Digital Image Watermarking Techniques and Applications: A Survey",International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 3, ,pp 533, March 2016

©IJRASET: All Rights are Reserved