An Extensive Literature Review on Digital Image Watermarking

Abhilasha Malviya, Asst. Prof. Nitin Lonbale
M-Tech Research Scholar, Department of Electronics & Comm.
Shri Balaji Institute of Technology & Management, Bhopal

Abstract:- In this review research work our have analyzed Watermarking techniques, grayscale image (logo) is used as watermark. In watermark embedding process, both the host image and watermark image are transformed into DWT domain where their coefficients are fused according to a series combination rule that take into account contrast sensitivity characteristics of the HVS. The method repeatedly merges the watermark coefficients strongly in more salient components at the various resolution levels of the host image which provides simultaneous spatial localization and frequency spread of the watermark to provide robustness against different attacks. Watermark extraction process requires original image for watermark extraction. In spread spectrum based watermarking technique, a visually recognizable binary image is used as watermark. In watermark embedding process, the host image is transformed into DWT domain.

Keywords:- Digital Image Watermarking & DWT.

I. INTRODUCTION

A secret imperceptible signal is embedded into the original data in such a way that it remains present as long as the perceptible quality of the content is at an acceptable level. The owner of the original data proves his/her ownership by extracting the watermark from the watermarked content in case of multiple ownership claims. Digital watermark may be comprised of copyright or authentication codes, or a legend essential for signal interpretation. The existence of these watermarks with in a multimedia signal goes unnoticed except when passed through an appropriate detector. Common types of signals to watermark are still images, audio, and digital video.

Watermarking System

In this thesis, work has been carried out on digital watermarking. Throughout the rest of the report, watermarking refers to digital watermarking. To avoid the unauthorized distribution of images or other multimedia property, various solutions has been proposed. Most of them make unobservable modifications to images that can be detected afterwards. Such image changes are called watermarks. Watermarking is defined as adding (embedding) a watermark signal to the host signal. The watermark can be detected or extracted later to make an assertion about the object. A general scheme for digital watermarking is given in Fig. 1. The watermark message can be a logo picture, sometimes a visually recognizable binary picture or it can be binary bit stream. A watermark is embedded to the host data by using a secret key at the embedded [2].

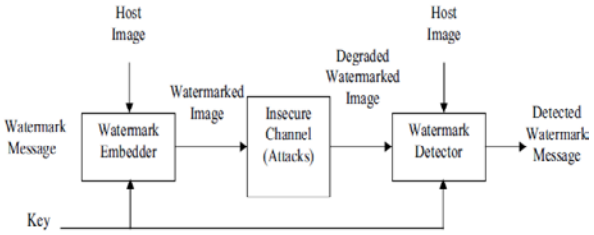

Fig 1 A Digital Watermarking System

The information embedding routine imposes small signal changes, determined by the key and watermark, to generate the watermarked signal. Only the owner of the data knows the key and it is not possible to remove the message from the data without the knowledge of the key. Then, the watermarked image passes through the transmission channel. The transmission channel includes the possible attacks, such as lossy compression, geometric distortions, any common signal processing operation and digital-analog and analog to digital conversion [5], etc. After the watermarked image passes through these possible operations, the message is tried to be extracted at the watermark detector. The decoding process can itself performed in two different ways. In one process the presence of the original unwatermarked data is required and other blind decoding is possible. The extracted watermark is compared with the original watermark (i.e. the watermark that was initially embedded) by a comparator function and binary output decision is generated. The comparator is basically a correlator. Depending on the comparator output it can be determined if the data is authentic or not. If the comparator output is greater than

equal to a threshold then the data is authentic else it is not authentic [8]

Watermarking Requirements

Watermark by itself is not sufficient to prevent abuses unless a proper protection protocol is established. The exact properties that a watermarking algorithm must satisfy cannot be defined exactly without considering the particular application scenario; the algorithm has to be used in. For example, in the video indexing application, evaluating the robustness of a watermarking scheme to any signal processing is meaningless, since there is no case that the video passes through some signal processing operation.

Imperceptibility

Watermarking algorithm must embed the watermark such that this does not introduce any perceptible artifacts into the host data and not degrade the perceived quality of the underlying host data. A watermark-embedding procedure is truly imperceptible if humans cannot distinguish the original data from the data with the inserted watermark [10].

Robustness

Robustness refers to the ability to detect the watermark, even if the quality of the host data is degraded, intentionally (malicious) or unintentionally (non-malicious). In general, there should be no way in which the watermark can be removed or altered without sufficient degradation of the perceptual quality of the host data so as to render it unusable.

Capacity

The capacity requirement of the watermarking scheme refers to be able to verify and distinguish between different watermarks with a low probability of error as the number of differently watermarked versions of an image increases [7].

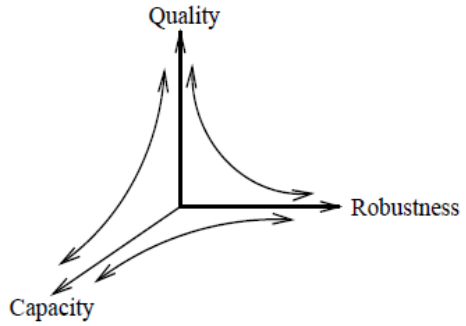

Fig. 2 Mutual dependencies between the basic requirements

II. SYSTEM MODULE

Throughout our discussion, our use $X(m,n)$ to denote the host image and $w(m,n)$ the watermark. The watermark, assumed to be a two dimensional array of real elements [3]. The watermark is visually recognizable binary or gray scale image. The size of the watermark is N×N. It is required that the size of the watermark in relation to the host image be "small". our assume, without loss of generality, that the watermark is smaller than the host by a factor of M 2, where M is an integer greater or equal to 1.

Watermark Embedding Method

The technique is comprised of the 3 main stages is summarized, the image and watermark both are decomposed using the DWT [8]. In the second stage, the watermark is selectively and repeatedly merged using a model of human contrast sensitivity to determine the most salient localized host image components. Last, the inverse DWT is applied to form the watermarked image. The following is the more detailed and analytic description of the procedure.

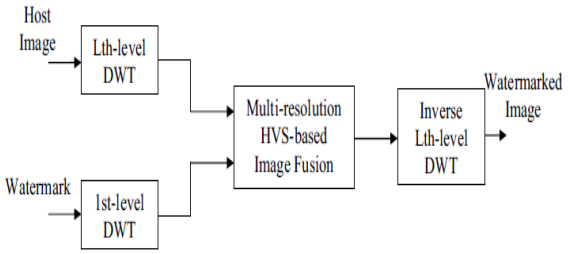

Fig. 3. The Fusion-Based Watermark Embedding Method

III. LITERATURE REVIEW

In the year of 2013 Bhupendra Ram.,[1] Investigated on Digital watermarking has been proposed as a viable solution to the need of copyright protection and authentication of multimedia data in a networked environment, since it makes possible to identify the author, owner, distributor or authorized consumer of a document. In this research work a new watermarking technique to add a code to digital images is presented: the method operates in the frequency domain embedding a pseudo-random sequence of real numbers in a selected set of DCT coefficient. And a new method for digital image watermarking which does not require the original image for watermark detection. The watermark is added in select coefficients with significant image energy in the transform domain in order to ensure non- erasability of the watermark. Advantages of the proposed method include: improved resistance to attacks on the watermark, implicit visual masking utilizing the time-frequency localization property of wavelet transform and a robust definition for the

threshold which validates the watermark.. Experimental results demonstrate that this proposed technique is robust to most of the signal processing techniques and geometric distortions.

In the year of 2013 Nagarjuna, P.V.; Ranjeet, K., [2] presented a stationary wavelet transform based digital image watermarking algorithm is proposed. The proposed algorithm combines the information of low frequency SWT coefficients and the watermark image without any change in the information present in the original image. Key is combination and is used to extract the watermark. The proposed method will not affect the quality of the image because of no change in the information present in the original image. The simulation results demonstrate the effectiveness of the proposed algorithm.

In the year of 2013 Sharifara, A.; Rahim, M.S.M.; Bashardoost, M.[3] proposed on introduce a novel approach to preserve digital images' copyrights. Hence as ISB scheme was selected in relation to the approach in an attempt conquer the issues of robustness and imperceptibility in watermarked imagery. According to the literature review, embedding the aimed secret bits (Watermark) is a problematic issue inside a host image (normal 8-bit, grey-scale) in a sense to make it undetectable by the HVS (Human Visual System) in addition to the matter that it is predicted to receive any attacks. The suggested method here represents an improved scheme for the embedding of ISB which maintains the robustness and cultivates the rate of security by employing repeated bits in various bit planes over an irregular order and it develops the LSB technique specifically in circumstances where robustness and imperceptibility are main points of assessment.

In the year of 2013 Thongkor, K.; Mettripun, N.; Pramoun, T.; Amornraksa, T.,[4] described a situation where the copyright of distributed images/photos in social networks is violated. Since the images/photos published on social networks are usually modified and/or compressed to the match the template provided by the service providers, our thus propose a digital image watermarking based on DWT coefficients modification to be used for such images/photos. Basically, in the embedding process, the blue component of original host image is decomposed by the Discrete Wavelet Transform (DWT) to obtain the coefficients in LL subband, and some of them are used to carry watermark signal. In the extraction process, original coefficients prediction in the LL sub-band based on mean filter is employed to extract the embedded watermark. The experimental results show that the performance of our proposed method in term of average NC is superior to the previous ones.

In the year of 2013 Alkhathami, M.; Fengling Han; Van Schyndel, R.,[5] researched on a new digital watermarking technique for fingerprint images using the Dual-Tree Complex Wavelet Transform (DTCWT). The watermark is embedded into the real and imaginary parts of the DTCWT wavelet coefficients. This work focuses on the study of watermarking techniques for fingerprint images that are collected from different angles without corrupting minutiae points. our investigate the effect of the watermark on the fingerprint features after the watermark embedding process. Veri Finger V5.0 is used to determine the matching score between the template and the watermarked images. The users identity is linked with the fingerprint features to add more authentication factors to the authentication process. The SHA2 hash function is used to encode the user identification number by generating the hash value and convert it into a binary image to construct the watermark data. The original fingerprint image is not required to extract watermark data. The proposed method has been tested using the CASIA fingerprint image database with 500 fingerprint images from 100 persons.

IV. PROBLEM FORMULATION

The first challenge concerns Watermarking techniques can be used for the transmission of secrete private messages. Since various governments restrict the use of encryption services, people may hide their messages in other data. Although not yet widely recognized as such, bandwidth-conserving hybrid transmission is yet another information embedding application, offering the opportunity to re-use and share existing spectrum to either backwards-compatibility increase the capacity of an existing communication network, i.e., a “legacy” network, or allow a new network to be backwards-compatibility overlaid on top of the legacy network. In this case the host signal and embedded signal are two different signals that are multiplexed, i.e., transmitted simultaneously over the same channel in the same bandwidth, the host signal being the signal corresponding to the legacy network. Unlike in conventional multiplexing scenarios, however, the backwards compatibility requirement imposes a distortion constraint between the host and composite signals.

V. CONCLUSIONS & FUTURE SCOPE

Primarily focus on to provide good tradeoff between perceptual quality of the watermarked image and its robustness to different attacks. For this purpose, our have

discussed two digital watermarking algorithms in discrete wavelet domain (DWT) by incorporating contrast sensitivity based human visual system model (HVS). One is fusion based watermarking, and other is spread spectrum based watermarking. our used grayscale watermark for fusion based watermarking, and binary watermark for spread spectrum based watermarking. Through computer simulation, our analyzed the performance of the algorithms against different attacks such as JPEG compression, AWGN noise, mean and median filtering, cropping, and image resizing. The important points to conclude from the simulation analysis for fusion based watermarking algorithm were our conclude that the both the methods are robust against different non geometric attacks. However, both the methods fail for non-geometric attacks such as rotation or affine transformations.

The discussed watermarking algorithms are robust to non-geometrics attacks only. our can extend this work by developing new watermarking algorithms, which are robust to both geometric attacks and non geometric attacks. Future work will also concentrate on making the watermarking methods more practical by modifying the techniques such that the host image is not required to extract the watermark and robust to both geometric and non geometric attacks.

REFERENCES

[1] Bhupendra Ram.," Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform," International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013.

[2] Nagarjuna, P.V.; Ranjeet, K., "Robust blind digital image watermarking scheme based on stationary wavelet transform," Contemporary Computing (IC3), 2013 Sixth International Conference on , vol., no., pp.451,454, 8-10 Aug. 2013.

[3] Sharifara, A.; Rahim, M.S.M.; Bashardoost, M., "A Novel Approach to Enhance Robustness in Digital Image Watermarking Using Multiple Bit-Planes of Intermediate Significant Bits," Informatics and Creative Multimedia (ICICM), 2013 International Conference on , vol., no., pp.22,27, 4-6 Sept. 2013.

[4] Thongkor, K.; Mettripun, N.; Pramoun, T.; Amornraksa, T., "Image watermarking based on DWT coefficients modification for social networking services," Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2013 10th International Conference on , vol., no., pp.1,6, 15-17 May 2013.

[5] Alkhathami, M.; Fengling Han; Van Schyndel, R., "Fingerprint image watermarking approach using DTCWT without corrupting minutiae," Image and Signal Processing (CISP), 2013 6th International Congress on , vol.03, no., pp.1717,1723, 16-18 Dec. 2013.

[6] Mothi, R.; Karthikeyan, M., "A wavelet packet and fuzzy based digital image watermarking," Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on , vol., no., pp.1,5, 26-28 Dec. 2013.

[7] Channapragada, R.S.R.; Prasad, M.V.N.K., "Digital watermarking algorithm based on complete complementary code," Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on , vol., no., pp.1,4, 26-28 July 2012.

[8] Akbarzadeh, M.R.; Ghofrani, S., "Image content authentication and tamper localization based on semi fragile watermarking by using the Curvelet transform," TENCON 2012 - 2012 IEEE Region 10 Conference , vol., no., pp.1,6, 19-22 Nov. 2012.

[9] Van Schyndel, R.G., Tirkel, A.Z., and Osborne, C.F., "A digital Watermark." Proc. of the IEEE Int. Conference on Image Processing. Vol. 2, (1994): pp. 86-90.

[10] Swanson, M.D., Kobayashi, M., and Tewfik, A.H., "Multimedia Data-Embedding and Watermarking Technologies." Proc. of the IEEE. Vol. 86, No. 6, (June 1998): pp. 1064– 1087.

[11] Petitcolas, F., Anderson, R., and Kuhn, M., "Information Hiding - a Survey." Proc. of the IEEE. Vol. 87, No. 7, (July 1999): pp. 1062–1078.

[12] Barni, M., Bartolini, F., Cox, I.J., Hernandez, J., and Perez-Gonzalez, F., "Digital Watermarking for Copyright Protection: A communications perspective." IEEE Communications Magazine. Vol. 39, No. 8, (August 2001):pp. 90–133.

[13] Langelaar, Gerhard C., Setyawan, I., and Lagendijk, R.L., "Watermarking Digital Image and Video Data: A state-of-the-art-overview." IEEE Signal Processing Magazine. Vol.17, No. 5, (September 2000): pp. 20-47.

[14] Voyatzis, G., Mikolaides, N., and Pitas, I., "Digital watermarking: An overview." Proc. of IX European Signal Processing Conference(EUSIPCO), Island of Rhodes, Greece. (September 8-11, 1998): pp. 13-16.

[15] Wolfgang, R.B., Podilchuk, C.I., and Edward J. Delp, "Perceptual Watermarks for Image and Video." Proc. of the IEEE. Vol. 87, No. 7, (July 1998): pp. 1109-1126.

[16] Cox, I.J., Miller, M.L., and Bloom, J.A., "Watermarking Applications and their Properties." Proc. of IEEE Int. Conference on Information Technology, Las Vegas. (March 2000): pp. 6-10.

[17] Craver, S., Memon, N., Yeo, B.-L., and Yeung, M.M., "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications." IEEE Journal On Selected Areas in Communications. Vol. 16, No. 4, (May 1998): pp. 573-586.