International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Survey on Fragile Digital Watermarking

Dr. Dayanand .G Savakar[1], Shivanand Pujar[2]

[1]Associate Professor, Department of Computer Science, Rani Channamma University, Post Graduate Centre, Vachana Sangama-Toravi, Vijaypura-586108, Karnataka,India

[2]Research Scholar,Department of Computer Science, Rani Channamma University, Belgavi-591156, Karnataka,India

Abstract: ***Several major research fields have been identified in case of digital image processing and in information security , one among them is the digital watermarking. It has got the ability to make a stronger ownership of the original data and also can completely retain the original data from the watermarked data. This characteristic feature is considered to be the most essential part of some of the important media, such as medical and military images and these kinds of media do not allow any of the information part to be lost. There exist various kinds of watermarking schemes as well as techniques which are used for wide range of applications. But still there is a chance to analyse and determine the requirement of a watermarking scheme with respect to the attributes like; fidelity and capacity in the areas like content based watermarking, tamper detection, multiple watermarking etc., by devising new schemes and algorithms. There is also a need for an effective watermarking system that has to be introduced. The requirements are application-dependent, but some of them are common to most practical applications. In this article, we discuss about need for effective watermarking process and watermark retrieval process, keeping in the mind the basic properties; Fidelity and Capacity.***

Keywords: Capacity, Fidelity, Fragile, Semi-Fragile.

1. Introduction

The computers act as the main sources in the field of Image Processing and Pattern Recognition techniques. Steganography and Digital watermarking etc are the fields those are responsible to accomplish tasks like information hiding using image processing techniques which can be noticed in recent developments. Stegnography is referred to as an alternative tool for privacy and security. The primary goal of this stegnography is to hide the fact that a covert communication is present within an innocuous communication. Further the primary goal of steganalysis is to detect when a covert communication is occurring. Since steganographic and digital watermarking algorithms can be built on a shared foundation of data-hiding principles but the desired properties of stegnographic and steganalysis systems are quite different from those of digital watermarking. The effectiveness of embedding of a watermarking system measures the probability of an error when the detector is applied immediately after embedding but prior to any subsequent distortion. Further their might be instances that this error rate might be non-zero and indicates the fact that limitations imposed on the embedder may prevent successful embedding of all bits. However, it is expected that watermarks have to undergo image-processing manipulations like rotation, scaling, image compression and image enhancement without causing any changes in their attributes. Further the data is incorporated into an image that is capable enough to verify its authenticity or the identity of the owners watermarking. The visible digital watermarking is the one if the watermark information that is embedded into the picture can be seen into it; if it is not visible then it is called as invisible digital watermarking. If the base signal is copied, then the embedded watermark information is also carried into the copy. Further a base signal is capable to carry a number of different watermarks into it at a specific time period. Digital Watermarking is known to be a major sector of research in the fields of Image Processing and Pattern Recognition. Further Digital Watermarking is utilised in cases like - Copyright protection, Source tracking (different recipients get differently watermarked content), Broadcast monitoring (television news often contains watermarked video from international agencies), Covert communication etc. The copyright of digital images are being widely protected by using Digital Watermarking. In order to strengthen the intellectual property right of a digital image, a trademark of the owner could be selected as a watermark and embedded into the protected image. The image that embedded the watermark is called a watermarked image. Then the watermarked image could be published, and the owner can prove the ownership of a suspected image by retrieving the watermark from the watermarked image. According to the retrieved results, we can determine the ownership of the suspected image. Generally, a practical and useful watermarking scheme has to meet the following requirements.

- **Imperceptibility**:

The degradation in quality within the original image as well as within the watermarked image should not exit. This property is called imperceptibility. A watermark can be incorporated within an image as either visible or invisible. The visible watermark is perceptible and is similar like a noise. It can be removed by using any of the noise removing process. To reduce the risk of cracking, the watermarking schemes those are proposed are all invisible. One more criteria that has to be satisfied is the quality of the watermarked image is should not be changed. If the watermark embedding process seriously damages the quality of the watermarked image, the watermarked image will draw the attention of attackers or even lose its value.

- **Fragile watermarking**

A fragile watermark is a mark that is readily altered or destroyed when the host image is modified through a linear or nonlinear transformation. Fragile image watermarking is a technique to detect tampering and to authenticate digital image. This concept of fragile watermarking came into

existence while ensuring the legitimacy and data integrity especially when it is utilised as evidence in case of court or in case of medical diagnosis. Further this fragile watermarking technique can be classified into two broad categories as:
a) Block Wise fragile watermarking
b) Pixel wise fragile watermarking

In case of block –wise fragile watermarking the host image is divided into a number of small blocks and watermark information is derived from the vital content of block of the host image. When the image is altered the tampered block and watermark contained in that block will mismatch and by this inequality one can easily identify the tampered block. Block wise fragile watermarking has some limitations like within a particular block some pixels are really altered and some are not which is somewhat undesirable. In case of pixel-wise fragile watermarking watermark information is derived from gray value of pixels and further embedded into image itself. Any alteration in any of the gray value of pixel will be responsible for wrong value of watermark in further calculation at receiver side hence one can easily recognize altered pixel with high precision.

- **Embedding and Retrieving:**

The watermark must be able to be easily and securely embedded and retrieved by the owner. Therefore, the overheads of embedding process and retrieving is as shown from the below figure.1 conventional and reversible watermarking schemes process should be limited in a reasonable range. In recent years a special kind of digital watermarking is discussed widely, called reversible watermarking. It not only provides the protection of the copyright by embedding the assigned watermark into the original image but also can recover the original image from the suspected image. The retrieved watermark can be used to determine the ownership by comparing the retrieved watermark with the assigned one. There are two types of watermarking schemes are practiced. If the process does not require the help of original image to retrieve the watermark then the process is called to be as the blind. Since some of the conventional watermarking schemes require the help of an original image to retrieve the embedded watermark and are called to be as non blind watermarking. However, the reversible watermarking can recover the original image from the watermarked image directly. Therefore, the reversible watermarking is blind, which means the retrieval process does not need the original image.

- **Semi-fragile watermarking**

Semi-fragile watermarking techniques aim at detecting malicious manipulations on an image, while allowing acceptable manipulations such as lossy compression. Further semi-fragile methods are robust to incidental modifications such as JPEG compression, but fragile to other modifications such as high impact additive noises. That is, some incidental image manipulations have to be considered allowable during the process of media transmission and storage, while other malicious modifications from attackers should be rejected. Semi-fragile watermark is a mechanism for implementing selective authentication. It describes a watermark that is unaffected by legitimate distortions, but destroyed by illegitimate distortions.

- **Higher Embedding Capacity**

The capable size of information that is capable enough to embed is defined as the embedding capacity. Due to the reversible watermarking schemes having to embed the recovery information and watermark information into the original image, the required embedding capacity of the reversible watermarking schemes is much more than the conventional watermarking schemes. The embedding capacity should not be extremely low to affect the accuracy of the retrieved watermark and the recovered image. The steps of conventional watermarking and reversible watermarking are similar except there is an additional function to recover the original image from the suspected image. Therefore, the reversible watermarking is especially suitable for the applications that require high quality images such as medical and military images. In addition, there are two research fields often connected with digital watermarking: data hiding (Steganography) and image authentication. The purpose of data hiding is using the cover image to conceal and transmit the secret information. And the purpose of image authentication is to verify the received image whether it be tampered or not. In order to achieve the goals, the data hiding scheme should have a large embedding capacity to carry more secret information, and it has to be imperceptible to keep the secret undetectable. The image authentication schemes also require embedding some information into the protected image, and also has to keep the imperceptibility between the preprocess image and processed image. The imperceptibility, high embedding capacity, readily embedding and retrieving, and blind are the basic criterions of the reversible watermarking. A reversible data hiding scheme and a reversible image authentication scheme can be also defined as the schemes which can recover the original image from the embedded image.

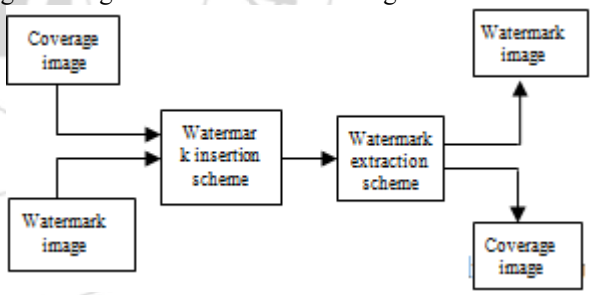

Figure 1: Proposed Methodology

From the above figure.1 initially the watermark is being incorporated within the original image/within the cover image that is under test using some of the watermark insertion scheme. The process leads to the creation of suspected image to identify the watermark for any of the following reasons like authenticity, copyright protection and so on. The result may leads to either conventional process or to the reversible process. In case of conventional process only the watermark is retained were as in case of reversible watermarking original image along with the watermark is retained. Further depending upon the sensitivity of the watermark, these watermarks are identified to be as the active watermarks and passive watermarks. And also depending upon the type of watermark incorporated the scheme can be identified to be as the highly-fragile, semi-fragile, and also the capacity of the cover image to incorporate the maximum

size of the watermark can be defined. Based upon these criteria's it is possible to carry out further work on single level multiple image watermarking scheme, multiple level single image watermarking scheme, and multiple image multilevel watermarking schemes.

2. Literature Survey

(C.kailasanathan ,2003) proposed a paper that describes about a scheme based on fragile watermarking for authenticating images based on the Yeung-Mintzer scheme. The scheme prevents the two main attacks proposed for Yeung-Mintzers scheme. It also analyse the security level with respect to other attacks. Performance is evaluated by carrying out the attacks on the watermarked image like blurring, embossing, oil-painting, rotation at one-degree,etc. The security level of the scheme and the possible extension to multiple watermarking scheme are also investigated. (Raja' S. Alomari and Ahmed Al-Jaber, 2004) proposed a paper that describes about an algorithm by the name Secure Fragile Watermarking Algorithm which are mainly used in building Content Authentication Systems. Further this algorithm is an extension of an existing data hiding scheme which is proposed for binary images. The proposed algorithm shows that a very high data payload to fidelity trade-off. It is a logical consequence since at most two bits are flipped when embedding number of bits equal to block size. The proposed content authentication has a very high level of security this is accomplished due to the existence of the weight and key matrices used in embedding algorithm and the presence of hash key in the hashing function. (Xinpeng Zhang and Shuozhong Wang, 2008) proposed a scheme based upon novel fragile watermarking which is capable of recovering the original image from its tampered version. In this scheme a watermark consisting of reference-bits and check bits is embedded into the host image using data hiding method. By comparing the extracted bits and calculated check-bits one can identify the tampered image-blocks. (Kai Wang et al,.2008) proposed a scheme for authenticating 3D semi-regular meshes using fragile watermarking. The inserted watermark is robust to the so-called content preserving attacks including vertex reordering and similarity transformations. The main objective is to check the integrity of the mesh. It is the first algorithm on this topic that is robust to all the content-preserving attacks providing a precise attack localization capability. (Shan Suthaharan, 2010), have proposed a technique for an efficient fragile image watermarking for pixel level tamper identification and its resistance. The technique uses mainly five most significant bits of the pixels to generate watermark bits and embeds them in the three least significant bits. The paper also presented two new algorithms related to nonaggressive and aggressive tamper detection algorithms. (Hammed khataeimaragheh and Hassan Rashidi. 2010) proposed a paper that describes a scheme to detect, localize, and recover from malicious modifications within the relational databases using a novel fragile watermarking technique. The proposed scheme carries out a technique of dividing all the tuples of a database into a number of groups then watermark are being embedded in to the individual group. Security analysis is also carried out that shows a number of difficulties for an attacker to modify the database without affecting the embedded watermarks.(Xiaojun Qi and Xing Xin, 2011) presents a paper for image content authentication and tampering localization which is based upon novel semi-fragile watermarking scheme. This scheme utilizes a method known as non-traditional quantization method. The method begins with the extraction of watermark using the results of the parity of quantization from the probe image. Further the construction of binary error map and the computation of two authentication measures is carried out. Finally the two measures are integrated to confirm the image content and to localize the tampered areas. Based upon the experimental results it is declared that the scheme undergoes four peer schemes and has the capability to identify intentional tampering and incidental modification along with localizing tampered regions. (Xiaojun Qi and Xing Xin, 2010) presents a paper for image content authentication and tampering localization which is based upon novel semi-fragile watermarking scheme. This scheme utilizes a method known as non-traditional quantization method. The method begins with the extraction of watermark using the results of the parity of quantization from the probe image. Further the construction of binary error map and the computation of two authentication measures is carried out. Finally the two measures are integrated to confirm the image content and to localize the tampered areas. Based upon the experimental results it is declared that the scheme undergoes four peer schemes and has the capability to identify intentional tampering and incidental modification along with localizing tampered regions. (Shivendra Shivani et al., 2011) proposed a paper that signifies an approach to a block-wise fragile watermarking that is based on k-medoids clustering. According to the proposed algorithm image is divided into the blocks and forty eight bits are calculated for each block, consisting of forty five recovery bits and remaining three authentication bits. The forty eight bits of each block are mapped with a secret key. The result can be noted by comparing extracted and calculated authentication bits and rectifying the tampered block and extracted recovery bits from mapping blocks gives sufficient information to recover extensive content of host image. (Dr.M.Mohamed Sathik and S.S.Sujatha, 2012) proposed a paper in which a semi-fragile watermarking technique which embeds watermark signal into the host image in order to authenticate it. In this case the watermark is generated as a binary pattern from the feature of the host image and is embedded in the high frequency sub band in the wavelet domain. PSNR as well as SR are computed to measure image quality. The designed method makes use of the Arnolds Transform for scrambling the watermark and there by offers higher security. (Shelvie Nidya Neyman et.al,. 2013) this paper proposes a scheme that detects and locates the modification of the data with higher accuracy further ensures the exact recovery of the original content. Further a scheme known as reversible data-hiding is introduced based on the idea of difference expansion with Manhattan distances. This scheme cannot only verify the integrity of the vector map, but also accurately locate the modification to certain features. (Young-Long Chen et al, 2013) proposed a technique to protect intellectual property rights and also provides security and protection using fragile watermarking. The paper also uses the logistic map with the parameter u=4 to generate chaotic dynamic behaviour with

the maximum entropy1. It uses Arnolds Cat Map Encryption Algorithm. (Prabhishek Sing and R S Chadha, 2013) proposed a paper that defines complete definition of watermarking and the associated concepts like different categories of watermarking process further signifies which watermarking process should be used. The proposed paper gives an idea of comparative analysis of some major watermarking techniques. (Mohammed S. Khalil et.al, 2014) Proposed a scheme that describes about two layers embedding scheme, the first layer of watermarking method is applied on wavelet domain and second layer on spatial domain. The paper approaches mainly a novel watermarking method to facilitate the authentication and along with the detection of the image forgery on the Quran images. The technique of discrete wavelet transforms are applied to decompose the host image into wavelet prior to embedding the watermark in the wavelet domain. Further A chaotic map is utilized to blur the watermark to make it secure against the local attack. Experiment results shows that the proposed methods are fragile and have superior tampering detection even though the tampered area is very small. (Rohit Thanki and Komal Borisagar,.2015) proposed a paper that describes about the fingerprint watermarking technique that is based on SVD and Compressive Sensing theory which is further proposed for the protection of biometric template at the system database of a multibiometric system. (Krisda Khankasikam,. 2015) proposed a scheme describing about a new fragile watermarking technique which was developed within the wavelet domain and is based on the discrete wavelet transform and Arnold's scrambling algorithm. (Pooja Loni et.al 2015)proposed a paper that describes the reductions of the limitations associated with the irreversible and reversible schemes along with the different parameters.Further the limitations associated with the vector quantization and transplantation attacks are addressed. (Taha Basheer Taha and Mohamed T.Sultan, 2015) proposed a paper that describes about wavelet based digital watermarking algorithms, which is capable enough to detect the alteration within the images and to protect the copyright of the image. Thus the proposed algorithm is termed to be semi-fragile watermarking.Further the algorithm shows high sensitivity for content altering and robust against safe altering like changing file format. (Yu-Cheng Fan and Yu-Yao Hsu, 2015) presents a scheme of novel fragile watermarking which is based upon artificial neural network (ANN). Without the intervention of the original image, whenever the image is subjected to any kind of modifications, these alterations can be noticed via the fragile watermark. Hence depending upon the type of alterations carried out it is possible to know what kinds of modifications are being done on the image. Further based upon the declared experimental results it could be seen that the proposed method also identifies tampering and detect the exact location of the tampering along with the kind of alteration that has taken place. Further the proposed method displays a high recognition ratio detecting the different types of modifications.(Pragya Jain and Anand S.Rajawat) proposed a paper from which a number of results are reported from the comparative study on various related as well as relevant aspects of the digital watermarking mainly image authentication techniques those are based on fragile watermarking and fuzzy clustering and also genetically inspired watermarking techniques used mainly for integrity verification.

3. Conclusion

According to the literature survey it can be noted that several watermarking schemes and techniques are devised for wide range of applications. Still there is huge scope for the analysis and determination of the suitability of a watermarking scheme with respect to the properties like; fragile watermarking, fidelity and capacity. Destroying the watermark by any of these types of distortions, like loose compression, filtering, resizing, contrast enhancement, cropping, and rotation and so on, by developing suitable methodologies. Reduction of false-negative (the probability of failing to detect the embedded watermark) / positive-error (detecting the watermark without its presence) in the absence of attacks or signal distortions, detecting malignant transformations, tamper detection & recovery can be addressed by introducing novel scheme using masking techniques (embed information in significant areas) so that the hidden message is more integral to the cover image than just hiding it in the noise level. A number of secret hiding techniques show that the fact, that the HVS (Human Visual System) is sensitive to small amplitude changes either in the spatial or frequency domain. Thus, there is a need for devising an algorithm to consider the sensitivity of HVS to colour changes, edge changes, contrast changes, texture changes, and so on by using either any of the features like low-level features (computed from pixels) or high level features (like - Region of Interest).

References

[1] C.Kailasanathan, "Fragile Watermark based on polarity of pixel points", 3rd International Symposium on Image and Signal Processing and Analysis, vol.2, pp. 860-865, 2003.
[2] Raja'S Alomari and Ahmed Al-Jaber, "A Fragile Watermarking Algorithm for Content Authentication", International Journal of Computing and Information Sciences, Vol.2, no.1, pp.27-37, 2004.
[3] Xinpeng Zhang, Shouzhong Wang, "Fragile Watermarking With Error-Free Restoration Capability", IEEE Transactions On Multimedia, Vol.10, no. 8, pp.1490-1499, 2008.
[4] Kai Wang, Guillaume Lavoue, Florence Denis and Atilla Baskurt, "A Fragile Watermarking Scheme for Authntication of Semi-regular Meshes", The EUROGRAPHICS Associations, 2008.
[5] Shan Suthaharan, "Logistic Map-Based Fragile Watermarking for Pixel Level Tamper Detection and Resistance", EURASIP Journal on Information Security, Vol. 2010, pp.1-7, ISSN:1687-4161, 2010.
[6] Hamed Khataeimaragheh and Hassan Rashidi, "A Novel Watermarking Scheme for Detecting and Recovering Distortions In Database Tables", IJDMS, Vol.2, No.3, pp.1-11, 2010.
[7] Xiaojun Qi and Xing Xin, "A quantization-based semi-fragile watermarking scheme for image content authentication", Journal of Visual Communication and

Image Representation, ISSN:1047-3203, pp:187-200, 2010.

[8] Shivendra Shivani, Sushila Kamble, Anoop Kumar Patel and Suneeta Agarwal, "Image Authentication and Restoration Using Block-Wise Fragile Watermarking based on k-Medoids Clustering Approach", Proceedings of International Journal of Computer Applications, pp. 44-50, 2011.

[9] Dr.M.Mohammed Sathik and S.S.Sujatha, " Authentication of Digital Images by using a semi-Fragile Watermarking Technique", International journal of Advanced Research in Computer Science and Software Engineering, vol.2, Issue.11, pp.39-44, 2012.

[10] Pragya Jain and Anand S.Rajawat, "Fragile Watermarking for Image Authentication", Intrnational journal of Electronics and Computer Science Engineering, Vol.1, pp:1232-1237, 2012.

[11] Shelvie Nidya Neyman, Benhard Sitohang and Sobar Sutisna, " Reversible Fragile Watermarking Based on Difference Expansion Using Manhattan Distances for 2D Vector Map", The 4th international Conference on Electrical Engineering and Informatics, Procedia Technology vol.11, pp.614-620, 2013.

[12] Young-Long Chen, Her-Terng Yau and Guo-Jheng Yang, " A Maximum Entropy-Based Chaotic Time-Variant Fragile Watermarking Scheme for Image Tampering Detection", Entropy, Vol.15, pp.3170-3185, ISSN 1099-4300, 2013.

[13] Prabhishek Singh and R S Chadha, " A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT) , Vol.2, Issue. 9, pp.165-175, 2013.

[14] Mohammed S.Khalil, Fajri Kurniawan, Muhammed Khurram Khan and Yasser M.Alginahi, "Two-Layer Fragile Watermarking Method Secured with Chaotic Map for Authentication of Digital Holy Quran", The Scientific World Journal, Vol. 2014, Article ID. 803983, pp1-29, 2014.

[15] Rohit Thanki and Komal Borisagar, " Multibiometric Template Security Using CS Theory –SVD Based Fragile Watermarking Technique, WSEAS Transactions on Information Science and Applications, vol.12, pp.1-10,E-ISSN:2224-3402, 2015.

[16] Krisda Khankasikam, " A New Fragile Watermarking Scheme Based on Wavelet Edge Feature" ,International Journal of Future Computer and Communication, Vol..4, No.4, pp.270-274, 2015.

[17] Pooja Loni, V.S.Malemath, Sushma Chaugule and Anup Kalyanshetti, "A Study on Reversible Fragile Image Watermarking Scheme", International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, Issue.8,ISSN.2278-1021, pp.436-441, 2015.

[18] Taha Basheer Taha and Mohamed T.Sultan, " Wavelet-Based Semi Fragile Watermark for Digital Images", International Journal of Emerging Engineering Reasearch and Technology, vol.3, Issue.4, pp.75-80, 2015.

[19] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, "Digital Watermarking and Stegnography", ISBN 978-0-12-372585-1.

[20] Yu-Cheng Fan and Yu-Yao Hsu , " Novel Fragile Watermarking Scheme using an Artificial Neural Network for Image Authentication", Applied Mathematics and Information Sciences An International Journal.9, No.5, pp.2681-2689, 2015.

Author Profile

Dr. Dayanand G. Savakar is having 24 years of teaching and 10 years of research experience, he has completed his B.E degree from Karnataka University Dharwad, post graduation M.S from Birla Institute of Technology and Ph.D from Visvesvaraya Technological University., Belgaum, India. He is now working as Associate Professor, in the Department of Computer Science, Rani Channamma University, India. He has published more than 24 research articles in international journals/conferences. Currently he is guiding three Ph.D candidates. His areas of interests are – Image Processing, Pattern recognition and Information security.

Mr. Shivanand Pujar is having 1 year 6 months of teaching experience, he has completed his B.E degree in ISE from Basaveshwara Engineering College Bagalkot and post graduation M.Tech in computer science and engineering from Reva Institute of technology and management Bangalore under Visvesvaraya Technological University, Belgaum, India. He is now an research scholar in the Department of Computer Science, Rani Channamma University, Belgaum, India.