International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 03 (MAY-JUNE, 2016)

A Survey for applied Attacks on Digital Watermarking Methods, DCT & RW

Ravish Dhurve[1], Prof. Lokesh Malviya[2]
Computer Science & Engineering Department
Sam College of Engineering & Technology, India
[1]ravish.dhurve123@gmail.com, [2]lokesh.031986@gmail.com

Abstract-A digital watermarking technique has been planned as a possible resolution to the need of copyright protection and authentication of transmission info in a very networked setting, it makes possible to identify the author, owner, approved consumer of document victimization DWT technique were developed in recent years. As a result of it'll recover the watermarked info back to the primary host signal; reversible watermarking algorithms are suitable for medical, military and completely different special fields. This paper proposes a reversible element technique watermarking rule supported LSB replacement. It cannot solely recover the primary info to a high extent, but even have robust strength and low hard quality and .The watermark is superimposed in select coefficients with important image energy at intervals the transform domain therefore on make sure non- eras ability of the watermark. Benefits of the technique improved resistance to attacks on the watermark, hidden visual masking utilizing the time-frequency localization property of wave transform .Digital image watermarking that does not need the primary image for watermark detection and purpose reversible technique is robust to most and ownership.

Keywords—Watermarking, Visibility, Security, Robustness, Reversible data hiding, discrete cosine Transform.

I. INTRODUCTION

The development of information technology and communication network, multimedia technique has been applied to many related fields. The confidentiality, integrity and availability (CIA) of multimedia information, as the fundamental properties, are easily damaged in signal processing and transmission process because of the vulnerability and the external environment. Therefore, it is essential to search for some effective methods to deal with these problems. Digital watermarking has provided a valid solution to this problem. Image, audio or video marks can be embedded into digital contents for the purpose of content authentication, copyright protection, forensic tracking, counterfeit deterrence, multimedia indexing, etc. Now a day, billions of bits of information bring into existence in every half a second. And due to great acceptance of the Internet along with expeditious evolution of multimedia technology, users have more likelihood to use digital data (image, video and audio files, web publishing digital repositories and libraries). After all copying a digital data is very easy and fast, problems like, protection of rights of the content and proving ownership, arises. Digital watermarking is a solution to these problems as it has various applications like copyright protection, authentication, secret communication, and measurement. E-commerce, E-voting, medical safety, broadcasting monitoring, military and indexing can be protected by digital watermarking [1].Watermark remains intact to the cover image even if it is copied, is the characteristic of watermarking. Hence to certify ownership of data watermark is extracted and tested. Digital watermarking is the course of action of embedding a watermark in a multimedia object. This object may be image, audio, video and any digital content for the purpose of information hiding. Powerful watermarking technique should be selected for strong watermark embedding. According to type of document like text, image, audio, video used for watermarking, various techniques are used. Depending on human perception these techniques are classified as visible and invisible methods of watermarking. According to application source based and destination based watermarking techniques are used whereas on the basis of domain in which the watermark is inserted, two categories are made i.e., spatial-domain, and transform-domain methods [1]. Inserting the watermark into the spatial-domain component of the cover image is a direct method. It is easy to implement and requires less computations [1]. But the basic problem in watermarking in spatial domain is that the watermark is more susceptible to attacks than transform domain [2]. Whereas ,magnitude of coefficients in a transform domain are modulated, while embedding watermark in the transform-domain techniques such as discrete cosine transform(DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD) [3].

International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 03 (MAY-JUNE, 2016)

Transform-domain methods provide more information embedding and more robustness against many common attacks. But the computational cost is bigger than spatial-domain watermarking techniques.

1.1Type of image watermarking

Digital image watermarking has fall under into three categories accordingly based on the different watermarks:

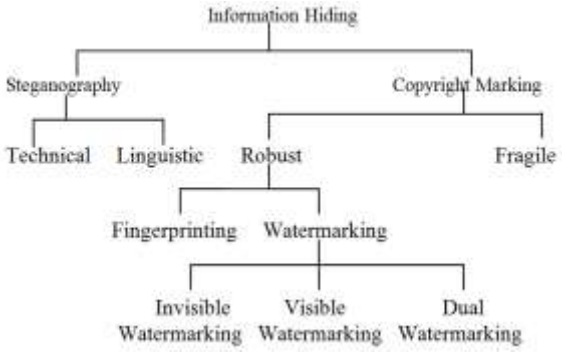

Fig: 1 Classifications of Digital image Watermarking

1. Visible Watermarks-These are the logos concept enlargement. These sorts of watermarks are solely applicable for the pictures. A transparency criterion evolves once these logos are embedded into the still pictures. The watermarks happiness to the current class is exhausting to get rid of or alter once cropping attack falls.

2. Invisible Watermarks -As the name clears its which means the watermark should be hidden from the surface world. The detection of those sorts of watermark will solely be done by the upper authority or agencies. The watermarks happiness to the current class is utilized by the author authentication or creator or possession and for locating the unauthorized person.

3. Fragile Watermarks- These are known as by the name of the tamper proof watermarks. The watermarks happiness to the current class is shattered by the info management. The image while not watermark indicates that a trial has been created on the initial image and forgery has evolved within the absence of watermark.

1.2 Watermarking Techniques

Watermark can be applied either in spatial domain or in frequency domain as shown in Figure 2. In Spatial domain, the watermark is applied by modifying pixel values of the host image while the transform coefficients are altered for embedding watermark in frequency domain [5]. Frequency domain is widely used, in comparison to spatial domain due to its robust nature and maintaining the imperceptibility of original image intact.

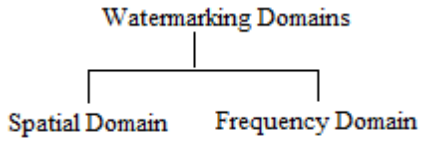

Fig2 Domains of Watermarking

1.2.1 Spatial Domain

Two commonly used techniques in spatial domain are: Correlation based technique and Least Significant Bit Modification scheme [4]. This technique is conceptually simple and uses less computational intricacies, hence, suitable for video watermarking where real-time performance is prime goal. However, it is incompetent to attacks, poor imperceptibility and less robust [8].

1.2.2 Frequency Domains

Commonly used transforms are Discrete Fourier Transformation (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).

1.2.2.1 DCT **:-** In DCT, middle frequency bands are the primarily focused zone for watermark embedding after dividing the original image/video frame into sub-bands of lower and higher resolutions. It can be implemented in O (n log n) operations, thereby, giving faster results. It can overcome attacks such as low pass filtering, blurring, sharpening, but weak against attacks such as rotation, cropping or scaling. Few of the applications where DCT is applied include fingerprint identity, employee i-cards, pan cards, or medical imaging areas [5].

1.2.2.2 DWT: - In DWT, the image is divided into sub images in hierarchical fashion [5] as lower (LL) and higher resolutions (Horizontal HL, Vertical LH and Diagonal HH) frequency bands. DWT supports multi-resolution characters; hence, it is widely used. Few of the applications where DWT is widely used include government applications, military applications, bank applications or broadcast monitoring [4]. DWT coefficient's magnitude is smaller for other higher bands (HH, LH, and HL) [6] [7] and is larger in the lowest bands (LL) at every decomposition level. Embedding watermarks in lower frequency bands leads to enhanced robustness to attacks.

1.2.2.3 DFT: - In DFT, continuous functions are converted into frequency components [4]. It is robust against geometric attacks such as scaling, translation, cropping and rotation. It is better than DCT, DWT or spatial domain as they are not robust and invariant to geometric attacks.

1.3 Applications of Digital Watermarking

Owner Identification: It establishes ownership of the content. Copy Protection: It prevents people from making illegal copies of copyright content. Authentication of Content: To detect modifications of the content as a sign of invalid authentication. Fingerprinting: Trace back illegal duplication and duplication of the content. Broadcast Monitoring: Especially for advertisements and in entertainment industries, to monitor content that is broadcast as contracted and by the authorized source. Medical Applications: Used to provide both authentication and confidentiality without affecting the medical image in any way.

II. LITERATURE SURVEY

Nirupama [9] "Digital Watermarking uses DWT and DES", proposed an algorithm to protect digital data by embedding watermark that is encrypted by DES algorithm. Two level discrete wavelet transformation (DWT) is applied to the original image before apply watermarking in it.

Mei Jiansheng [10] "A Digital Watermarking Algorithm Based on DCT and DWT". Introduce a discrete wavelet transform digital watermark algorithm based on human vision characters. In this technique, first of all watermark image is transformed by using DCT transformation. Then this watermark image is embedded into the high frequency band of wavelet transformation domain.

Chih Chin Lai [11] "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition" proposes a new technique in which the watermark is not embedded directly on the wavelet coefficients but rather than on the elements of singular values of the cover image's DWT.

Rey [12] "A Survey of Watermarking Algorithms for Image Authentication" identifies some of the emerging techniques of that time. They introduced the notion of image content authentication so that they can easily detect image tampering. They also highlighted the features about effective authentication scheme. They proposed an approach using feature based watermarking to show that an image is authentic even though the content has been modified.

Manoj Ramaiya [13] "Fingerprint Recognition based on Minutiae Extraction Principle", Proposed a method that is created for fingerprint recognition based on minutiae.

Navnidhi Chaturvedi [14] "Digital Watermarking using Discrete Wavelet Transform". In this paper have compared watermarking using DWT & DWT-DCT method's performance analysis on basis of PSNR.

Zhang [15] "Separable Reversible Data Hiding in Encrypted Image", in this literature survey, reversible data hiding technique is used to increase the hiding capacity which is based on histogram shifting. This approach is used for two predictor's methods such as center prediction method and JPEG-LS median edge predictor (MED) method. From the experimental results, the terms of embedded capacity and PSNR value has proposed the scheme outperforms some of the previous works. Finally, the results provided to prove that the PSNR value and embedded capacity of the proposed scheme are better than that of previous literatures for signal-level, multi-level and the computation complexity of the proposed scheme. It is also very small as it just deals with the shifting and searching operations. The advantage of this paper is the Simple Less computation and drawback is data compression is not efficient.

Md. Bilal Husain [16] "A New Approach of Image Encryption Using 3D Chaotic Map to Enhance Security of Multimedia Component", this survey has discussed about a 3D chaos based simple encryption technique with combination of position permutation techniques and value transformation techniques. For image encryption technique is not a new concept of pixel position permutation and XOR operation for value transformation. This algorithm is use for low, medium and high security purpose by controlling its complexity.

Xiaolong [17] "General Framework to Histogram Shifting-Based Reversible Data Hiding ", the proposed research is based on a Reversible Data Hiding concept by using Histogram Shifting method. In this method after shifting the pixels of the host image in a predefined order with the help of Histogram, the data which is to be hidden is embedded into the host or

cover image. The data is smoothly recovered by reversing the shifting process, after embedding the data pixels in the host image. So the data can be recovered very easily without any loss in the data. On the receiving side, the original image perfectly restored and the hidden message can be extracted. This paper construct a general framework to HS-based RDH is proposed. According to this framework, one just needs to define the shifting and embedding functions and then to obtain a RDH algorithm, we facilitate the design of reversible data hiding. Furthermore, by incorporating this framework with the help of PEE and pixel selection techniques, they are also introduced two novels of RDH algorithms. So the proposed framework has a potential to provide RDH algorithms. However, the proposed framework may design different RDH algorithms. Some HS-based algorithms such as the one based on adaptive embedding and the location-map-free methods cannot be derived by the proposed framework.

Dr. Mohammad V. Malakooti [18] A Lossless Secure Data Embedding In Image Using DCT and Randomize Key Generator, In this paper presents a new algorithm of Lossless Secure data embedding algorithm in which the vital information can be embedded into the cover image while maintaining the security of the data to be embedded and preserving the quality of cover image. Here, during the process of the data embedding that are need to be considered the two main issues of cover image quality and embedded data security. SDEM-DCT (Scramble Data Embedding in Mid-frequency range of DCT) Algorithm consists of three major security levels. This level can be used to hide Credit Card Numbers of many customers inside the bank LOGO. It proposes a high capacity data hiding method. Also introduce a robust Scramble and Descramble Data embedding algorithms which name it MK randomize key Generator to have a more Security for embedded data. This method is securer than most of its predecessors. Finally, the results show that our method indeed that provides acceptable image quality and adjustable embedding capacity. Also show the distortion of the stego-image caused by this method at low embedding capacity is the same as that by other same algorithms.

Nallagarla Ramamurthy [19] “Effect of Various Attacks on Watermarked Images” Watermarked images are affected by various attacks such as cropping, salt & pepper noise and rotation. These attacks destroy the inserted watermark, so that the copyright problem may arise. The effect of these attacks can be reduced by properly inserting the watermark with effective algorithm. In this paper, a blind transform domain based algorithm using Radial Basis Function Neural Network is introduced. The proposed algorithm is robust to cropping, salt & pepper noise and rotation attacks compared to other algorithms.

III. PROPOSED SOLUTION

3.1 Problem Declaration

Data requirement is increasing day by day. Even after progress in technology in storage density the demand is difficult to achieve. Uncompressed media data consume a lot of memory and are therefore bulk of such data is difficult to store and transmit. Images contribute to the maximum storage requirements in the present world. Both storage and transmission time is affected. Hence image compression is need of the hour. Compression of images reduces the size of the memory required for storing the image. When we compress images, inner details have to be compromised but that increases our motive of storage and transmission to great extend. Multimedia based applications have created a need for better and efficient ways to encode signals (images). One of the main problems and the criticism of the DCT is the blocking effect. In DCT images are broken into blocks 8x8 or 16x16 or bigger. The problem with these blocks is that when the image is reduced to higher compression ratios, these blocks become visible. This has been termed as the blocking effect.

2.2 Proposed method

Proposed Watermarking Technique an image watermarking using reversible pixel method based on bits replacement .Revisable pixel is a process standard image divide into matrix and bits replace in the technique for embedding data into a digital host image. Data extraction is actually the reverse process of the data embedding. the watermarked image not only can well hide the watermark information by storing the bits replacement into the host image .The algorithm can make a job in robust and computational complexity also good. A study paper in the field of digital watermarking and identify various outcome. It is data of the host image can be recovered and reliable. It is provide strong & robustness. It is provide best possible data hiding ability. It is providing data authentication.

IV. CONCLUSION

A watermarking algorithm based on the secondary LSB replacement, DCT-DWT and SVD which allows near

lossless recovery of the original host image. This algorithm not only can recover the original host image to a high extent, but also have good performance in robustness, hiding ability and computing complexity. The embedding capacity of this algorithm is mainly decided by the ratio between the size of the host image and watermark. Also, the main defect of this algorithm is the low embedding capacity, the algorithm may fail. Future job will be focused on improving the reversibility and performance of the algorithm.

REFERENCES

[1]. Chih-Chin Lai, Member, IEEE, and Cheng-Chih Tsai," Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE, Vol. 59, No. 11, November 2010.

[2]. Shahin Shaikh, Manjusha Deshmukh, "Digital Image Watermarking In DCT Domain", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013 .

[3]. Ruizhen Liu and Tieniu Tan, "A SVD Based Watermarking Scheme For Protecting Rightful Ownership*", Multimedia IEEE Transitions, ISSN 1520-9210 Vol. 4, Issue 1.

[4]. Ekta Miglani, Sachin Gupta "Digital Watermarking Methodologies - A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.

[5]. Radhika v. Totla, K. S. Bapat, "Comparative Analysis of Watermarking in Digital Images Using DCT & DWT", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.

[6]. Ying Zhang, Jiqin Wang, Xuebo Chen, Watermarking Technique Based On Wavelet Transform for Color Images, IEEE, 2012.

[7]. Qing Liu, Jun Ying Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis", IEEE, 2012.

[8]. Dr. Nasseer Moyasser Basheer, Shaimaa Salah Abdulsalam, "Watermarking Algorithm in DWT using HVS Characteristics", The Fourth Scientific Conference of the College of Computer Science & Mathematics, Iraqi Journal of Statistical science 2011.

[9]. N. Tiwari, M. K. Ramaiya and M. Sharma, "Digital Watermarking using DWT and DES".

[10]. J. Mei, S. Li and X. Tan, "A Digital Watermarking Algorithm Based on DCT and DWT", International Symposium on Web Information Systems and Applications Nanchang, May 22-24, pp. 104-107, 2009.

[11]. C. C. Lai and C.-C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 11, November 2010.

[12]. C. Rey, J.L. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication", EURASIP Journal on Applied Signal Processing, 6, pp. 613 – 621, Hindawi Publishing Corporation 2002.

[13]. Prof. M. Ramaiya, "Fingerprint Recognition based on Minutiae Extraction Principle".

[14]. M. Narang and S. Vashisth, "Digital Watermarking using Discrete Wavelet Transform", International Journal of Computer Applications (0975 – 8887), vol. 74, no. 20, July 2013.

[15]. Zhang, "Separable Reversible Data Hiding in Encrypted Image**",** IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, April 2012.

[16]. Md. Billal Hossain, Md. Toufikur Rahman, A B M Saadmaan Rahman, Sayeed Islam,**"** A New Approach of Image Encryption Using 3D Chaotic Map to Enhance Security of Multimedia Component", 3rd International Conference On Informatics, Electronics & Vision 2014.

[17]. Xiao long Li, Bin Li, Bin Yang, and Tieyong Zeng ,"General Framework to Histogram Shifting-Based Reversible Data Hiding ", IEEE Transactions On Image Processing, Vol. 22,No. 6, June 2013.

[18]. Dr. Mohammad V. Malakooti, Mehrzad Khederzdeh,'" A Lossless Secure Data Embedding In Image Using DCT and Randomize Key Generator" IEEE 2012.

[19]. Nallagarla Ramamurthy, Dr. S. Varadarajan, "Effect of Various Attacks on Watermarked Images", IJCSIT, Vol. 3, 2012.