ROBUST DIGITAL WATERMARKING FOR IMAGES: REVIEW

Saloni Singla, Deepak Sharma

MTech, Computer Science Department, KITM, Kurukshetra University, Haryana, India

Head of department, Computer Science Department, KITM, Kurukshetra University, Haryana, India

ABSTRACT

Digital Image Watermarking used for protecting digital media files and data. It has been an active research field since last decades. Digital Image watermarking is an approach that enables a user from being misused of personal images or information. Here, the term "watermarking" refer to data hiding for copyright protection and image security. Digital Watermarking is becoming a necessity these days for various reasons such as duplication, modification and manipulation of images .In this paper, we have discussed various techniques that enable users to allow a security over their images and data, thus providing a secure transfer of digital files. The main issue in protecting our image files is to secure our data and important information from being viral or open to all, thus making its end to end retrieval that is only required end user is able to access that data.

KEYWORDS: Watermarking,PSO,Image processing.

1. INTRODUCTION:

When photos are posted online, they are rarely protected, meaning they can be used by anyone who has access to them. Photos can be protected through copyrights, but a trick often used by photographers is to watermark their photos. Traditionally, watermarks were variations in the thickness of a paper that can only be seen in certain light conditions. Digital watermarks are text or logos that are put on top of the image to establish the owner of the photo. Often, watermarks are opaque and look indented. A great way to ensure that no one is using photos without your permission is to add a watermark with Google's Picasa or Adobe Photoshop.

Digital watermarking, a new technology for data protection and intellectual property right verification, provides a promising way of protecting multimedia data from illegal manipulation and duplication.

For example, a watermark can be a tag, label or digital signal. A host may be multimedia object such as audio, image or video but here we will take into consideration the images only.

The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include electronic advertising, realtime video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest towards developing new copy deterrence and protection mechanisms. One such effort that has been attracting increasing interest is based on digital watermarking techniques. Digital watermarking is the process of embedding information into digital multimedia content such that the information can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, development and commercialisation.

2. RELATED WORK:

- **Palak Patel et al [1]** proposed that with the rapid advancement in WWW(World Wide Web), digital network, digital library services, information can be retrieved anytime. Therefore, security of information has become a major issue. Securing this information while communication over channels was necessary. A need for developing technology that would help in securing the information called Steganography was introduced. The way of hiding some important or private, data or information within something that appeared to be nothing out of the normal. Nowadays the term "Information Hiding" relates to both watermarking and steganography. So steganography and digital watermarking have been combined together to hide and secure image with watermark logo inside cover image. For this purpose, DCT, DWT, SVD and RSA approach have been used. Using DCT, encrypted watermark logo (encryption performed using RSA) is hid inside an unsuspicious image, which results in Stego image. This Stego image is hidden inside cover image using DWT and SVD. This approach was used to transmit secure information like movie with their respective image, copyright information of company, finger-print or thumb impression of particular person. These methods have used for security purpose which would be beneficial for overall security to nation.

- **Aniyan, et al[2]** presented that digital watermarking technology has enabled the copyright protection and content authentication of digital multimedia data. His study involved experiments whose results showed that the developed method is robust against various attacks and potentially compatible with JPEG compression.

- **J. S. Tsai, et.al[3]** proposed a method for robust digital image watermarking. On the Selection of Optimal Feature Region Set for Robust Digital Image Watermarking in the year 2011, His study aimed to select a non-overlapping feature region set, which has the greatest robustness against various attacks and can preserve image quality as much as possible after watermarked. It first performed a simulated attacking procedure using some predefined attacks to evaluate the robustness of every candidate feature region. According to the evaluation results, it then adopts a trackwith-pruning procedure to search a minimal primary feature set which can resist the most predefined attacks. In order to enhance its resistance to undefined attacks under the constraint of preserving image quality, the primary feature set is then extended by adding into some auxiliary feature regions. The experimental results for StirMark attacks on some benchmark images support our expectation that the primary feature set can resist all the predefined attacks and its extension can enhance the robustness against undefined attacks. Comparing with some well-known feature-based methods, the proposed method exhibits better performance in robust digital watermarking.

- **S. Kuri, et.al[4]** proposed that communication of digital data over Internet has increased drastically as huge amount of multimedia data is embedded over Internet every day. Digital images contribute a major part of multimedia data. The rapid advances in computer network hardware and software has led to high risk of piracy. Therefore, there was a need of techniques for copyright protection and content authentication of digital images. Watermarking is one such technique. He concluded that a robust image watermarking technique in wavelet domain that uses the Pseudo Random Number (PRN) sequence generated using Elman neural network to watermark the image. The proposed method decomposed original image in the wavelet domain using discrete wavelet transform and watermarked it with a PRN sequence. The watermark was extracted to recover the original image. The neural network generated PRN sequence was a highly random sequence providing high level of security. This approach showed an excellent resistance against intensity transformation attack.

- **Furqan, et.al[5]** provided a framework for robust and blind digital image watermarking technique to achieve copyright protection. In order to protect copyright material from illegal duplication, various technologies had been developed, like digital watermarking. In digital watermarking, a signature or copyright message is secretly embedded in the image by using an algorithm. In this paper, it was implemented that algorithm of digital watermarking by combining both DWT and SVD techniques. Initially, we decompose the original (cover) image into 4 sub-bands using 2-D DWT, and then we apply the SVD on each band by modifying their singular values. After subjecting the watermarked image to various attacks like blurring, adding noise, pixelation, rotation, rescaling, contrast adjustment, gamma correction, histogram equalization, cropping, sharpening, lossy compression etc, we extract the originally inserted watermark image from all the bands and compare them on the basis of their MSE and PSNR values. Experimental results are provided to illustrate that if we perform modification in all frequencies, then it will make our watermarked image more resistant to a wide range of image-processing attacks (including common geometric attacks), i.e. We can recover the watermark from any of the four sub-bands efficiently.

- **Preeti Parashar et al[6]**, presented that security of multimedia like images, text, videos is a serious concern for the internet technology because of its being getting duplicated, distributed and manipulated easily. The digital watermarking is a concept of information hiding which hide the important information in non-crucial data for protecting illegal duplication and distribution of multimedia data. This paper provided a survey on the existing digital image watermarking techniques. The results of various digital image watermarking techniques had been compared on the grounds of the outputs. In the digital watermarking, the secret information are implanted into the original data for protecting the ownership rights of the multimedia data. The image watermarking techniques on the basis of domains like spatial domain or transform domain or on the basis of wavelets. The spatial domain techniques are worked upon the pixels and the frequency domain works on the transform coefficients of the image.This also elaborated and focused on the most important methods of spatial domain and transform domain and the merits and demerits of these techniques.

- **Meenu Singh et al[7]** announced that protection of multimedia and digital content is a must due to the rapid progress in internet technology and evolution of high speed networks. So, this has become a difficult task to protect copyright of an individual's creation. The purpose of digital watermarking is to protect important information within multimedia content to ensure a security of the concerned information. This paper then categorized the various watermarking techniques into various categories. It also provided the comparative study and analysis of these techniques that helped in knowing the positive and negative of these techniques. This comparison can further be used to improvise and propose various new techniques for the same.

- **Prabhishek Singh et al[8]** proposed that the expansion of the Internet has rapidly increased the availability of all form of digital data like audio, images and videos to the public. Digital watermarking is a technology being developed to ensure and facilitate all forms of protection of digital media like data authentication, security and copyright protection . This paper incorporated the detailed study of watermarking definition, concept and the main contributions in this field such as categories of watermarking process that explained which watermarking method should be used. It started with overview, classification, features, framework, techniques, application, challenges, limitations and performance metric of watermarking and a comparative analysis of some major watermarking techniques.

- **Neeraj Bhargava et al[9]** presented that these days, people are blindly using social networking sites for sharing their life moments as images or clicks as what we call. And the other side, users can access or even download those digital images easily. Fake people can exploit the original image by editing and modifying it which can then be uploaded and shared. The illegal use of personal image comes under copyright law. This research paper introduced a prototype for Digital Image Authentication System (DIAS). This system can perform visible and invisible watermarking on images. DIAS(Digital Image Authentication System) is applicable to color and gray images. The input image could be of any size, and the resultant image size would be same as input image. DIAS identified the ownership of digital image using Digital Watermarking. To hide and detect information from image, digital watermarking concept have been used which is the best way to copyright protection of the user. By using digital watermaking, the ownership can be blamed onto the fake person. This is known as an Authentication System for ownership identification. The complete system consists of two functions, one for hiding information inside image and other for detecting information from image. Here, results have been analyzed using Discrete Wavelet Transform (DWT) performed under digital watermarking.

- **Jaishri Guru et al[10]** proposed that the most significant property of digital information is that unlimited number of copies can be printed and distributed . It is required that unlimited number of perfect copies of text, audio and video that is produced illegally and distributed should be stopped and embedding copyright information and serial number in and video data. Today, internet is an essential channel for digital access, but it has been noticed that some people are misusing it by making illegal copies and leaking the audio information which creates a bad environment in the field of software industry .It can be protected by using digital watermarking which is very much in demand. It has been witnessed that the problem of protecting multimedia data becomes necessary and a lot of copyright owners are concerned about protecting any illegal duplication of their data or work. Some serious action needed to be performed in order to maintain the availability of multimedia data but, also the industry must come up with ways to guard intellectual property of makers, distributors or simple owners of such data . An approach known as digital watermarking is one that has received nearly all interest. The concepts like stenography and watermarking are main facts of quick developing area in case of information hiding. Generally, Watermarks are used where authentication or ownership is required that is a good way of confirming the ownership of multimedia. This paper attempted to first introduce digital watermarking as well as some of its necessary notions which is followed by describing some applications of watermarking techniques.

Table 1:Comparative study of recent Watermarking Techniques.

S.No.	Author's Name	Technique Used	Results
1.	Palak patel	Steganography, digital watermarking, DWT, SVD, DCT	Stego image using DWT and SVD
2.	Aniyan	Watermarking, JPEG compression, Discrete cosine transform	Robust image using JPEG compression
3.	J. S. Tsai	robust digital watermarking	Non-overlapping feature set to increase robustness
4.	S.Kuri	Robust Image Watermarking, PRN sequence, Neural Network, copyright protection, content authentication	Pseudo number generated to increase robustness of digital images
5.	A.Furqan	steganography, digital watermarks, authentication, copyright material, discrete wavelet transform (DWT), digital cosine transform (DCT), singular value decomposition (SVD), PSNR	Can recover watermark digital image from any four sub bands
6.	Preeti Parashar	Digital watermarking, Spatial domain, Least Significant Bit (LSB), Frequency domain, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT)	Concluded that images can be worked upon spatial domain and transform domain
7.	Meenu singh	Watermarking, DCT, DWT, Spatial Domain, Frequency Domain	Characterize various watermarking techniques to protect important information

8.	Prabhishek singh	Digital watermarking	Watermarking definition, concept and the main contributions in this field were found
9.	Neeraj Bhargava	Robust Watermarking; Color Images; Discrete Wavelet Transform (DWT)	Provided prototype for watermarking images
10.	Jaishri Guru	WaterMarking, Copyright Protection, DCT, LSB	Provided with some techniques of digital watermarking

3. CONCLUSION AND FUTURE SCOPE:

Nowadays, watermarking has become an important issue to protect suspicious information. In many papers mentioned above, techniques, approaches, frameworks have been found to protect information. This watermarking approach has a lot of future scope in a way it is used everywhere in the field where precious information is needed to be hidden.

4. REFERENCES:

[1]Palak Patel and Yask Patel, " Secure and authentic DCT image steganography through DWT – SVD based Digital watermarking with RSA encryption" published in Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on 4-6 April 2015.

[2] A. Aniyan and Deepa J , Electron. & Commun. Eng. Dept., Coll. of Eng., Alappuzha, India, J. Deepa "Hardware implementation of a robust watermarking technique for digital images" published in Intelligent Computational Systems (RAICS), 2013 IEEE Recent Advances, 2013.

[3] J.S. Tsai and Win-Bin Huang, and Yau-Hwang Kuo, Dept. of Comput. Sci. & Inf. Eng., Nat. Cheng Kung Univ., Tainan, "On the Selection of Optimal Feature Region Set for Robust Digital Image Watermarking", published in IEEE Transactions on Image Processing (Volume:20, Issue: 3), 2013.

[4] S.Kuri, Dept. of Electron. & Commun. Eng., KLS Gogte Inst. of Technol., Belgaum, India, V. B. Deshmukh ; G. H. Kulkarni, " Robust digital image watermarking using Pseudo Random Numbers", Proceedings of International Conference on Circuits, Communication, Control and Computing (I4C 2014), 2014.

[5] A. Furqan, Dept. of Electron. & Commun., Guru Gobind Singh Indraprastha Univ., New Delhi, India, M. Kumar, "Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using MATLAB", published in Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference, 2015.

[6] Preeti Parashar1 and Rajeev Kumar Singh2 PG Scholar1, Assistant Professor2 Department of CSE & IT, MITS, Gwalior, India, “A Survey: Digital Image Watermarking Techniques”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014), pp. 111-124, ISSN: 2005-4254 IJSIP Copyright ⓒ 2014 SERSC

[7] Meenu Singh, Abhishek Singhal and Ankur Chaudhary Department of Computer Science & Engineering, Amity School of Engineering & Technology Amity University, Uttar Pradesh, Noida, India, International Journal of Computer Science and Telecommunications [Volume 4, Issue 6, June 2013]

[8] Prabhishek Singh, R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks”,published in International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9ISSN: 2277-3754 ISO 9001:2008 Certified, March 2013.

[9] Neeraj Bhargava1, M.M. Sharma2, Abhimanyu Singh Garhwal3 and Manish Mathuria4, “Digital Image Authentication System Based on Digital Watermarking”,published in 2012 International Conference on Radar, Communication and Computing (ICRCC), SKP Engineering College, Tiruvannamalai, TN., India. 21 - 22 December, 2012. pp.185-189.

[10] Jaishri Guru1, Hemant Damecha2 Research Scholar M.E1, Assistent professor2 Software Systems - Department of Computer Science and Engineering Shri Ram Institute of Technology, Jabalpur R.G.P.V University Bhopal – India, “Digital Watermarking Classification : A Survey” , published in International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct 2014.