International Journal of Innovative Research in Technology & Science

ISSN: 2321-1156 Volume VIII Issue V, August-September 2020

A Survey on Enhanced Robustness Grayscale Image Hybrid Multiple Watermarking Technique

Ankit Choubey, Manish Rai
Department of CSE, RKDF, Bhopal, India
ankitchoubey90@gmail.com, manishrai2587@gmail.com

Abstract - *Digital watermarking technology may be a frontier research field, and it mainly focuses on the property rights, identification ion and authentication of the digital media to shield the essential documents. Consistent with the fundamental analysis of digital image watermarking the digital watermarking model consists of two modules, which are watermark embedding module and watermark extraction and detection module. Digital documents are often copied and scattered quickly to large numbers of individuals with none cost. People can download audio, image files, and that they can share them with friends and that they can influence or change their original contents. Because of this, there's more probability of the copying of such digital information. So, there's an urgent need of prohibiting such illegitimate copyright of digital media. Digital watermarking (DWM) is the dominant solution to the present problem. This paper aims to supply an exhaustive study of digital watermarking techniques primarily focuses on digital image watermarking DCT, and its applications used in many today in the real world. It had been supported the mixture of three transformations: the discrete wavelet transform (DWT), discrete cosine transform (DCT) and, the singular value decomposition (SVD) and also hybrid multiple watermarking techniques are low robustness and low PSNR. During this paper, three watermark images of sizes NXN, host image 512x 512, the effectiveness of the proposed method in terms of quality and robustness compared to other reported watermarking technique.*

Keywords: Digital Watermarking, Frequency Domain, DCT Coefficient, DWT, Attacks, Image Encryption, Image Decryption, Image Recovery, Robustness.

I. Introduction

The immeasurable attractiveness of the globe Wide Web in the early 1990s established the commercial potential of offering multimedia resources through digital networks. Since copying a digital data is extremely simple and swift too so, issues like, the shelter of rights of the content and proving ownership, arises. Digital watermarking has been anticipated. As one approach to hold out, this Digital watermarking came as a way and a tool to overcome shortcomings of existing copyright laws for digital data. Digital watermarking is a process during which owner identification (watermark) is embedded into the digital media at the sender end and later at the receiver end the embedded information is extracted to acknowledge the vital owner/identity of the digital content. Digital Image Watermarking is the process of insertion of image watermark in media content and its extraction, if required, for authentication or ownership verification of media content. A digital image watermark may be a piece of data that's hidden directly in media content, in such how that it's invisible to a person's observer [1] Differing types of watermarking methods for digital materials are developed that are classified into different categories depending upon the utilization and therefore, the requirement of data required for the extraction/detection of a watermark to see the authenticity of a digital content fragile watermarking is employed. In contrast, for the aim of copyright protection, robust watermarking is applied. This classification is application-dependent. Supported the knowledge required for the extraction/detection process watermarking schemes are often classified into blind, semi-blind, and non-blind categories. Also, another categorization is feasible depending upon the domain of Embedding of watermark: spatial and frequency. An in-depth review of watermarking schemes often used. The classifications of earlier developed approaches believe the area where critical information is going to be embedded and are further classified as [2].

1.1. Spatial Domain Techniques

In Spatial domain, the watermark directly embedded by modifying the pixels of the first image with none transformation of the picture. This system is usually fragile and applied within the pixel domain and has less complicated computation, thus consumes less time for archiving and retrieval. The smallest amount significant bit (LSB) technique is employed to embed information during a cover image. The LSB technique of a canopy image described by changing pixels by bits of the key message. An embedding scheme which randomly hides messages within the LSB of any/all component of the chosen pixel using a polynomial. If a polynomial is employed, the hacker must predict quite one number, i.e. all coefficients of the polynomial have got to be decoded correctly, and the probability of finding alright factors is a smaller amount compared to predicting single bit. Watermarking is often done by embedding watermark into sub-images with LSB technique. The watermarks usually embedded into specifics blocks of the host image where the choice of blocks predicated on entropy value which provides a high PSNR value. In [8], a unique, robust image watermarking scheme proposed for resisting geometric attacks. Watermark synchronization is first achieved by local invariant regions which may generate using scale normalization and image feature points. The watermark is embedded in all the local areas repeatedly in the spatial domain. During Embedding, each circular region first divided into homocentric cirque regions. Then the watermark bits are embedded by quantizing each cirque region into an odd or even region using odd-even quantization. Within the decoder, an odd-even detector (OED) to extract the watermark from the distorted image directly. By utilizing the generating principle and distribution feature of the D.C. (D.C.) coefficient, a unique blind watermarking algorithm proposed for colour host images in [9]. Firstly, the Y luminance of host image split into 8 × 8 sub-blocks, and therefore the D.C. coefficients of every block are directly calculated within the spatial domain. Secondly, consistent with the watermark information and therefore, the quantization step, the D.C. coefficients are calculated. Their increments further utilized to switch the values of all pixels within the spatial domain directly. When watermark extraction, only the watermarked image and therefore, the quantization step needed within the spatial domain. Low complexity and simple implementation are the benefits of spatial domain watermarking approaches. Despite these benefits, spatial watermarking methods are fragile against image processing operations [3].

1.2. Transformation Domain Techniques

Transformation of a picture is required to urge more information about the image and to scale back the computational complexity. Albeit this system takes longer and more complex than spatial domain technique, the embedded watermarked data can't be identified easily because of the previous procedure. In the transform domain, the watermark embedded after performing transformations like Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) etc. The watermark embedded within the transformed coefficients in comparison to spatial domain techniques these techniques offer high security and are robust to attacks. In the frequency domain watermarking, the values of selected frequencies often altered. Since high rates are going to be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to rates containing essential elements of the first picture [4]. DCT based Image watermarking is more robust as compared to the spatial domain watermarking techniques. DCT may be a fast transformation technique provides excellent energy compaction for highly correlated data, and most of the knowledge (D.C. coefficient) is within the first pixel. Proposes a robust watermarking approach supported the Discrete Cosine Transform (DCT) domain that mixes Quick Response (Q.R.) Code and chaotic system. When embedding the watermark, the high error correction performance and therefore the strong decoding capabilities of Q.R. Code are utilized to decode the text watermark information which improves the robustness of the watermarking algorithm. Then the Q.R. Code image is encrypted with a chaotic system to reinforce the protection of this approach. Finally, the encrypted image is embedded to the carrier image's DCT blocks after they underwent block-based Arnold scrambling transformation. During the extraction process, as long because the Q.R. Code image often decoded, the completeness and accuracy of the text watermarking information are usually guaranteed.

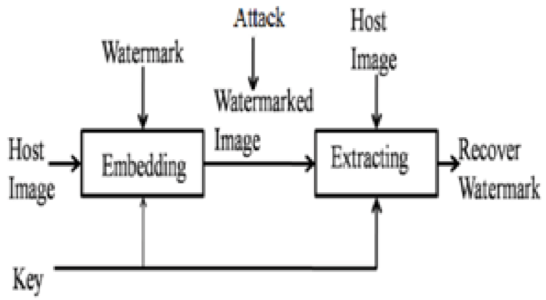

Figure 1 General block diagram of Embedding and extracting process of digital watermarking

In a replacement DCT based additive watermarking scheme proposed, which provides higher resistance to image processing attacks mainly JPEG compression. During this approach, the watermark embedded within the mid waveband of the DCT blocks only within the sub-band, which is carrying low-frequency components and therefore the high-frequency sub-band components remain untouched. A DCT based image watermarking framework proposed to reinforce the robustness of the watermark within the watermarked image against high-level lossy JPEG compression. Several proposed watermark frameworks in the previous0 couple of years have considered binary watermarks and watermark pixels directly embedded at the DCT coefficients of host images. Whereas during this framework used colour host images and grayscale watermarks and DCT performed on both the host image and watermark image. Watermark frequencies embedded within the DCT coefficients of the several blocks of the host images. A secret key's used that determines the embedding blocks of the host image [5].

II. Related Work

Srivastava et al. [6] Digital image watermarking are hiding information in any form (text, image, audio and video) in an original image without degrading its perceptual quality, which predicated on the Discrete Cosine Transform, Discrete Wavelet Transform and Singular Value Decomposition by using Arnold Transform method. DCT based watermarking techniques offers compression while DWT based compression provides scalability. Thus of these desirable properties are often utilized to make a replacement robust watermarking technique. The DCT coefficients of the DWT coefficients are wont to embed the watermarking information. So we choose SVD based digital watermarking which may be a method of authentication data embedding in image characteristics with the expectation to point out resiliency against different kind of unintentional or deliberate attacks. Here discrete wavelet transform plays the vital role of an efficient tool because of its multi-resolution capability. Alongside this wavelet transform, we error another powerful mathematical tool called the singular value decomposition (SVD). Though till date, both of them have individually used as a tool for watermarking of digital media, only a few works have utilized their skills in tandem, especially during this area. Our work focuses on using Direction Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) by employing a hybrid technology developed for the cover of the property with better robustness against the favoured malicious attacks. Thus we've seen practically by attacking the watermarked image against simulated attacks and recovering the brand from it.

Imran et al. [7] Digital Watermarking is an emerging field that aims to increase the advantages of authentication and copyright to digital media. These Watermarks remain hidden and don't degrade the standard of digital media. Different techniques used for incorporating watermarks into the media. Similar technologies are used at the receiver to retrieve watermarks. However, watermarks are vulnerable to attacks, and robustness, which quantifies the resilience to attacks, is a crucial property for all watermarks. However, in most cases, it's the appliance, that the watermarking is employed, that dictates the features that watermark should possess. During this paper, we've elucidated the techniques and applications of digital watermarking.

Patel et al. [8] because of the recent progress in the internet, digital contents, e.g. video, audio, images are widely used. Protection of digital materials must require. So, it's become a tough task to guard the copyright of a person's creation. Digital Image Watermarking aims to make sure and facilitate data authentication, security and copyright protection of digital images. This paper elaborates watermarking overview, embedding techniques, watermarking attacks, performance analysis. It'll be useful for researchers to implement active Image watermarking technique

Kaur et al. [9] this paper presents the challenges for a robust digital image watermarking algorithm. Need for copyright protection in digital media has led to enormous growth within the field of Digital Image Watermarking, whereby researchers are striving to return up with new ways of content protection. Recent developments within the field of watermarking though have provided new means of protecting data yet there are many factors which require to be addressed such the algorithm of embedding/ extracting a watermark is strong enough to satisfy these challenges. Robustness is often defined as resilience for a watermark to stay unaffected even when digital content is skilled in various processes and attacks and hence increase security, capacity, and imperceptibility of watermarked data. The paper begins with a quick introduction to cryptography and Steganography, which is the platform for a variety of digital watermarking concepts. Then, requirements for watermarking systems are discussed alongside methods to watermark data efficiently and their strengths and weaknesses. Last, there's a replacement method proposed which uses an idea of nested watermarks using Discrete Wavelet Transform for binary images and Cryptography using Spread Spectrum technique and is meant to be robust enough to cater to challenges presented here.

Jabade et al. [10] in image watermarking, information is embedded into cover media to prove ownership. Various watermarking techniques are proposed by many authors within the last several years, which include spatial domain and transform domain watermarking. Wavelet-based image watermarking is gaining more popularity due to its resemblance to the human sensory system. This paper elaborates suitability of wavelet transform for image watermarking; wavelet transform based image watermarking process, classification and analysis of wavelet-based watermarking techniques. This paper aims to supply a comprehensive review of the prevailing literature available on wavelet-based image watermarking methods. It'll be useful for researchers to implement effective Image watermarking method.

Yeung et al. [11] they propose a replacement method for invisibly watermarking high-quality colour and grayscale images. This method is meant to be used in image verification applications, where one is curious about knowing whether the content of a picture has been altered since some earlier time, perhaps due to the act of a malicious party. It consists of both a watermark stamping process which embeds a watermark during a source image and a watermark extraction process which extracts a watermark from a stamped image. The extracted watermark is often wont to determine whether the image has been altered. The processing utilized in the stamping and extraction processes is presented. We also discuss some advantages of this system over other invisible watermarking techniques for the verification application; these include a high degree of invisibility, colour preservation, simple decoding, and a high degree of protection against retention of the watermark after unauthorized alterations.

Hussein et al. [12] Digital watermarking techniques are developed to shield the copyright of digital media. This paper aims to supply an in-depth review and background about the watermarking definition, concept and therefore, the main contributions during this field. It begins with a digital watermarking overview, general framework, attacks, application, and eventually, a comprehensive survey of existing and most up-to-date watermarking techniques. We classify the methods according to various categories like host signal, perceptivity, robustness, watermark type, necessary data for extraction, processing domain, and applications. Within the survey, our main concern is an image only.

Li et al. [13] Watermark robustness to geometric attacks remains a challenging research field during this paper; a unique, robust image watermarking scheme is proposed for resisting such attacks. Watermark synchronization is first achieved by local invariant regions which may be generated using scale normalization and image feature points. The watermark is embedded in all the local areas repeatedly in the spatial domain. During Embedding, each circular region is first divided into homocentric cirque regions. Then the watermark bits are embedded by quantizing each cirque region into an "odd" or "even" area using odd-even quantization. Within the decoder, an odd-even detector (OED) is meant to extract the watermark from the distorted image directly. Localized Embedding achieves good invisibility, and repeated insertion enhances watermark robustness. Simulation results show that the proposed scheme is strong to both geometric attacks and traditional signal processing attacks.

Lang et al. [14] During this paper, we proposed a completely unique blind digital image watermarking algorithm supported the fractional Fourier transform (FRFT), which may be a generalization of the standard Fourier transform and its output has the mixed time and frequency components of the signal. The first image is segmented into non-overlapping blocks for watermarking, and every block is transformed by the two dimensional fractional Fourier transform with two fractional orders. Then each pixel value of binary watermark is embedded by modifying the back-diagonal FRFT coefficients of every image block at an equivalent location with a random array after performing an inverse two dimensional fractional Fourier transform; we will obtain the watermarked image, and therefore the transform orders are often considered because of the encryption keys during this method. A series of attacking experiments are performed on the proposed method. The tests results show that the proposed algorithm not only is of excellent imperceptibility and security and is exceptionally robust to JPEG compression noise attacks and image manipulation operations but can also provide protection even under compound attack.

Chang et al. [15]. Within the past few years, several digital watermarking schemes are proposed and supported DCT, DFT, and DWT transformations. During this paper, singular value decomposition (SVD)-based watermarking scheme is proposed. SVD transformation preserves both one-way and non-symmetric properties, usually not obtainable in DCT and DFT transformations. Within the proposed system, both of the D and U components are explored for embedding the watermark. Experimental results show that the standard of the watermarked image is good, which there strong resistance against general image processing is. Furthermore, the extracted watermark can still be easily identified after tampering.

III. Expected Outcome

The main objective of Digital watermark Robustness: The watermark should be ready to withstand after normal signal processing operations like image data secure transformation. Imperceptibility: The watermarked Image should appear as if the same because the original image to the traditional eye. The viewer cannot detect that watermark is embedded in it and eventually improve PSNR.

IV. Conclusion

The purpose of this paper is to present a survey of digital image watermarking approaches, one-bit position the watermark within the digital image just in case of space shortage problem. In recent years digital watermarking has achieved great deal attention. Distribution of images is now faster and easier via technology, especially on the web. They are concerned about illegal copying of their content. Watermarking techniques and hybrid, multiple watermarking techniques are standard image data or multimedia security on internet data transmission time. Watermarking DCT doesn't provide permanent protection, but it does not offer robustness, invisibility, data capacity and security. They need to offer various aspects of digital image watermarking in terms of overview, watermarking techniques, attacks, applications, performance analysis. Aside from it, a quick and comparative investigation of watermarking techniques is presented. It's concluded that the prevailing systems are often improvised to supply an error-resilient DCT architecture to compare other proposed method the prevailing architecture and to design, implement and validate DCT architecture and watermarking techniques using different standards image processing parameter. During this paper, they study the previous existing DCT approaches and that they found there are many issues which are associated with algorithm & architecture level. So during this area, there's many our proposed method where they will still make many improvements.

References

[1]. Jo, Minho, and HyoungDo Kim. "A digital image watermarking scheme based on vector quantization." IEICE Transactions on Information and Systems 85, no. 6 (2002): 1054-1056.

[2]. Liu, Yang, Shanyu Tang, Ran Liu, Liping Zhang, and Zhao Ma. "Secure and robust digital image watermarking scheme using logistic and RSA encryption." Expert Systems with Applications 97 (2018): 95-105.

[3]. Nikolaidis, Nikos, and Ioannis Pitas. "Robust image watermarking in the spatial domain." Signal processing 66, no. 3 (1998): 385-403..

[4]. Ratnakar, Viresh, Victor Ivashin, and Vasudev Bhaskaran. "Image transformations in the compressed domain." U.S. Patent 6,298,166, issued October 2, 2001.

[5]. Jiansheng, Mei, Li Sukang, and Tan Xiaomei. "A digital watermarking algorithm based on DCT and DWT." In Proceedings. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009), p. 104. Academy Publisher, 2009.

[6]. Srivastava, Shubham, and Arun Kumar. "Image Enhancement in Digital Image Watermarking Using Hybrid Image Transformation Techniques.", IOSR Journal of Electronics and Communication Engineering, ISSN: 2278-8735.Volume 11, Issue 3, Ver. II, PP 116-121, June 2016.

[7]. Imran, Sheikh, Ravinder Chaudhry, Junaid Gilani, and Suhail Nehvi. "The Techniques and Applications of Digital Watermarking." ,2014.

[8]. Patel, Jalpa M., and Prayag Patel. "A brief survey of digital image watermarking techniques." International Journal For Technological Research In Engineering 1, no. 7,2014.

[9]. Kaur, Deepti Prit, Jaspreet Kaur, and Kamal Deep. "Digital image watermarking: Challenges and approach for a robust algorithm." International Journal of Electronics Engineering 1, no. 1 95-97, 2009.

[10]. Jabade, Vaishali S., and Dr Sachin R. Gengaje. "Literature review of wavelet-based digital image watermarking techniques." International Journal of Computer Applications 31, no. 1: 28-35, 2011.

[11]. Yeung, Minerva M., and Fred Mintzer. "An invisible watermarking technique for image verification." In Proceedings of the international conference on image processing, vol. 2, pp. 680-683. IEEE, 1997.

[12]. Hussein, Ensaf, and Mohamed A. Belal. "Digital watermarking techniques, applications and attacks applied to digital media: a survey." threshold 5: 6, 2012.

[13]. Li, Lei-Da, and Bao-Long Guo. "Localized image watermarking in the spatial domain resistant to geometric attacks." AEU-International Journal of Electronics and Communications 63, no. 2: 123-131, 2009.

[14]. Lang, Jun, and Zheng-Guang Zhang. "Blind digital watermarking method in the fractional Fourier transform domain." Optics and Lasers in Engineering 53: 112-121, 2014.

[15]. Chang, Chin-Chen, Piyu Tsai, and Chia-Chen Lin. "SVD-based digital image watermarking scheme." Pattern Recognition Letters 26, no. 10 : 1577-1586, 2005.