

Improving Image Imperceptibility Based on Block Histogram Shifting Technique and SRDHHT

Shalini Soni¹, M. Tech. Scholar Department of CSE, TIT, RGPV, India; shalinisoni22@gmail.com

Prof. Aishwaryai Vishwakarma², A.P. Department of CSE, TIT, RGPV, Bhopal; aishwarya_vishwakarma@gmail.com

Abstract: Image processing processes our area and field with many problems, and with digital image data increasing rapidly from the exchange of digital data and the increased use of digital images, it is important to protect confidential image data from illegitimate access. Recently, more attention is given to reversible hidden data (RDH) in encrypted images, as it has the excellent property that the first image cover often overlaps to recover after the integrated data is extracted while protecting Image content as confidential. This procedure uses the differential pixel function to embed more data than other random partitions using the block-based image sharpness, filtering, and refining approach with single-level wavelet decomposition shift techniques to stop image distortion problems. Transforms the content of the last image into the content of another image object of equivalent size. The transformed image, which resembles the target image, is used because the "image is encrypted" and subcontracted to the cloud. Therefore, the cloud server can simply integrate data into the "encrypted image" using any RDH method for plain text images to propose a secure reversible watermark technique for digital images using histogram change methods. Additional security is provided through watermarks provided with encryption. The watermark is provided encrypted and sequenced before the image embedding is digital. In addition, the block-based technique is evaluated for greater watermark capacity. The technical results are compared with the idea of MSE and PSNR. In our experience, watermark data is integrated into the first images using the Mat simulation laboratories. This document is presented using the technique of the old EBHT method and our digital watermark image method with proposed histogram change supports special and frequency domains, showing that spatial domain techniques provide image watermark security and recovery Watermark with better PSNR values compared to a frequency domain Improved impeccability supports technical changes of histogram block and proposed techniques.

Keywords: change histogram, reversible watermark, hidden data, BHS, spatial location, watermark, human visual system, PSNR.

I. INTRODUCTION

Electronic commerce, usually referred to as e-commerce, is that the shopping for and commerce of product or service over electronic systems like the internet & different PC networks. Therefore the growth of e-commerce applications within the World Wide internet needs the necessity to extend the protection of information communications over the internet. To produce security to those applications encryption and knowledge activity techniques were introduced & developed. There are several approaches like Cryptography, Watermarking and Steganography to transfer the data/image to the supposed user at destination with no modifications. A watermark may be a secondary image that is overlaid on the first image and provides a method of protecting the image

[1]. With the event of recent digital technology illegal operation and illegal authorization of the digital product are more and more rampant. Illegal use, copyright impersonation and intentional tampering of digital product wide exist in industrial and non-commercial areas that end in the piracy drawback that greatly affects social development. Affects social development. However, traditional protection technology cannot effectively settle these current issues. Aimed toward these things, this paper provides some algorithms, particularly the digital image watermarking algorithmic rule supported wavelet transformation, using the imperceptions, robustness, security and watermarking. This algorithmic rule makes an attempt to enhance the protection and hardness of the watermarking data by choosing and decision making the embedded position and balances the contradiction between imperceptions and hardness by choosing the embedded intensity issue. This paper embeds the watermarking data into the initial pictures by Matlab simulation and employs several types of attack experiments to check the algorithmic rule. Experiments show that watermarking is often well extracted through several attacks are added, that prove the transparency, robustness, security and easy-to-extract characteristics of the watermarking. An image histogram may be a kind of histogram that acts as a graphical representation of the tonal distribution in a very digital image. It plots the number of pixels for every tonal price. By observing the histogram for a particular image a viewer is going to be ready to choose the complete tonal distribution at a glance [2].

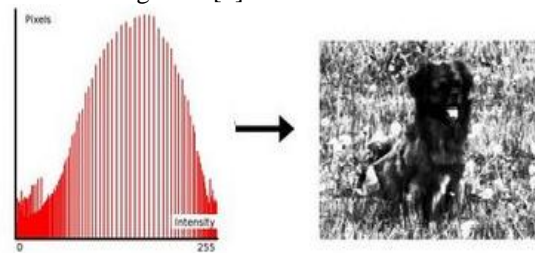


Fig1 Image as a Graphical Histogram Representation

Digital Image Data Hiding Frameworks

Digital watermarking systems usually include two primary components: the encoder and also the decoder. The inputs are the cover media knowledge, the embedding security key, and watermarks within the watermark encoder. The encoder inserts a machine-readable code (watermark) into audio, video, and pictures with variant embedding algorithms, conceptions, and schemes by modifying physical or electronic media and most watermarking procedures are controlled by non-public keys, that are assigned to the insertion and extraction procedure to extract the watermark data suitably and to warrant basic security. The outputs are the security key and also the watermarked contents within the watermark encoder. A watermark extractor or detector involves a two-step method. Watermark retrieval is that the opening that applies some scrambling algorithms to extract a sequence observed as retrieved watermarks. Then, within the second step, in digital watermarking the embedded

image watermark is detected and extracted original watermark from a suspected signal containing watermarks. The second step commonly needs the analysis and comparison of the unreliable watermark with the initial one, and also the consequences can be many types of confidence assessment displaying the similarity between the extracted watermark and also the original one. Digital Watermarking represents a good technique for authentication and ownership rights protections. It involves embedding [3].

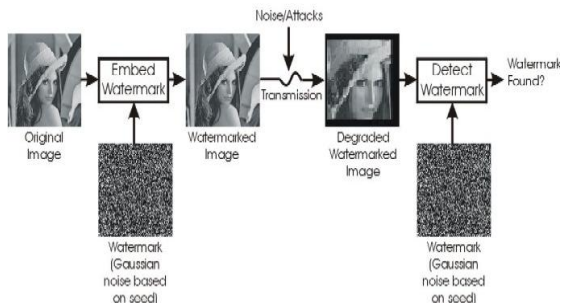


Fig 2 Digital Image Data Hiding frameworks Model

Digital Image Data Hiding Classification

Some of the necessary forms of watermarking supported completely different watermarks are given below

1. Visible watermarks: Visible watermarks are an extension of the thought of logos. Such watermarks are applicable to pictures only. These logos are inlaid into the image however they're clear. Such watermarks can't be removed by cropping the middle a part of the image.

2 Invisible watermarks: Invisible watermark is hidden within the content. It is often detected by an authorized agency only. Such watermarks are used for content and author authentication and for detection unauthorized duplicator.

3 Fragile watermarks: Fragile watermark also is called tamper-proof watermarks. Such watermark is destroyed by knowledge manipulation or in alternative words it's a watermark designed to be destroyed by any variety of repetition or encryption apart from a bit-for-bit digital copy. The absence of the watermark indicates that a replica has been created [4].

Needed Properties of Digital Image Data Hiding

Digital image watermarking issues to resolve some problems properly, thus, this paper highlights the most needs of watermarked image as following:

1. Robustness: The hardness is that the ability to detect the watermark once some signal process modification like spatial filtering, scanning, and printing, lossy compression, translation, scaling, and rotation, and alternative operations like digital to analog, analog to digital conversions, cutting, image improvement. Additionally, not all watermarking algorithms have a similar level of hardness, some techniques are strong against some manipulation operations, however, and that they fail against different stronger attacks. Moreover, it's not continuously desirable for the watermark to be strong, in some cases; it's desired for the watermark to be fragile. Therefore, the hardness is often classified as following [5].

i.Fragile: The watermark in this kind is meant to be destroyed at any reasonable modification, to observe any illegal manipulation, even slight changes, involving incidental and intentional attacks. Fragile watermarks are in the main utilized in content authentication and integrity

verification. They use blind detection sort because it is going to be mentioned in Detection varieties. Additionally, the implementation of fragile techniques is simpler than the implementation of strong ones [6].

ii. Semi-fragile: The watermark in this kind is strong against incidental modifications, however fragile against malicious attacks. And it's used for image authentication [7].

iii. Robust: The watermark is designed to be able to survive against incidental and intentional attacks. These types of watermarks are often used in broadcast observance, copyright protection, process, control management [8].

2. Imperceptibility: Imperceptibility (also referred to as invisibility and Fidelity) is that the most vital requirement in the watermarking system and it refers to the perceptual similarity between the first image before the watermarking method and also the watermarked image [5]. In alternative words, the watermarked image ought to look like the first image, and also the watermark should be invisible in spite of the occurrence of little degradation in image contrast or brightness. However, the challenge is that imperceptibility might be achieved, however, the hardness and also the capability are reduced, and vice versa, imperceptibility is also sacrificed by increasing the hardness and also the capability. Moreover, the watermark not continually desired to be invisible, sometimes, it's most well-liked to possess visible watermark into the image [8].

3. Security: Security is the ability to resist against intentional attacks. These attacks intended to alter the aim of embedding the watermark. Attacks varieties are often divided into 3 main categories: unauthorized removal, unauthorized embedding, and unauthorized detection [5]. Consistent with the precise usage of watermarking, the particular feature ought to be available within the watermark to resist the attacks. Therefore, for unauthorized removal, the watermark ought to be strong and to not be removed, and for unauthorized embedding (also referred to as forgery), the watermark ought to be fragile or semi-fragile to sight any modification. Lastly, for unauthorized detection, it ought to be an imperceptible watermark [9].

4. Capability: Capacity (also referred to as Payload) refers to the number of bits embedded into the image. The capability of a picture might be completely different consistent with the appliance that the watermark is designed for [5]. Moreover, finding out the capability of the image will show the USA the limit of watermark data that will be embedded and at a similar time satisfying the imperceptibility and hardness [10].

II. LITERATURE SURVEY

Cho et al. [11] proposed a fragile algorithm in the wavelet domain to authenticate semi-regular meshes. They first apply several wavelet decompositions on the original triangular mesh and then consider the facets in the obtained coarser mesh as authentication primitives. The basic idea is to slightly modify each facet so that the values of two predefined functions are the same, in order to make all these facets valid for authentication. Both function inputs are invariant to similarity transformations. However, it seems that two problems exist: first, the causality problem occurs because the modification of the current to be watermarked facet can influence the validities of its

already watermarked neighboring facets, and this problem is not mentioned by the authors; secondly, the watermark is inserted in a relatively coarse mesh obtained after several wavelet decompositions, which seems disadvantageous to provide precise attack localization capability.

Mohamed Ali Hajjaji et al. [12] proposed watermarking of medical image, in which a set of data is inserted in a medical image. The watermarking method is based on the least significant bits (LSBs) in order to check the integrity and confidentiality of medical information and to maintain confidentiality for patient and hospital data. For a 10% compression rate, the watermark is successfully recovered. The disadvantage of this technique is that all the substituted data cannot properly extract when a Gaussian noise is applied in the watermarked image.

Praun et al. [13] applied these decomposition and reconstruction methods for watermarking. They picked out the vertex split steps of the reconstruction process that introduced the most significant geometric modifications. For each vertex to be split in these selected steps, they defined a zone containing all its incident facets in the coarse mesh. They then found the corresponding area in the original dense mesh and took this area as the watermark carrier. One bit was inserted in each area by deforming it using a modulation function. Actually, their watermarking technique lies between spatial and classical spectral methods. Here, the multiresolution analysis serves to find the "low frequency", salient, spatial parts of the mesh and the insertion in these parts is supposed to be more robust. Unfortunately, these iterative edge collapse operations are still dependent on the mesh connectivity. Thus, this algorithm is non-blind mainly due to the connectivity recovery before extraction.

Maha Sharkas et al. [12] Senior Members IEEE, proposed a dual digital image watermarking technique for improved protection and robustness. They applied frequency domain technique (DWT) into the primary watermark image and then embedded secondary watermark in the form of a PN sequence. The resulting image is embedded into the original image to get the watermarked image. They applied compression, low pass filtering, salt and pepper noise, and luminance change attack into the watermarked image to increase the robustness of the technique. In all four attacks, the secondary watermark was detectable.

Meenakshi Sharma et al. [14], proposed the algorithm for the digital image watermarking method based on singular value decomposition, there are both of the L and U components are explored for the watermarking method. This method refers to the watermark embedding procedure. Also for watermark extracting procedure. The digital image watermarking method for copyright protection is robust. The experimental results show that the quality of the watermarked image is very good & there is strong resistance against many attacks. The image watermarking method help to achieves artificial intelligence. Digital image watermarking is the most effective solution in this & digital watermarking is used to protect the information that is increasing exponentially day by day. The results show that the quality of the watermarked image is better.

Koushik Pal et al. [15] proposed the biomedical image watermarking technique, a modified bit replacement

algorithm in the spatial domain, which is much better than the conventional simple LSB technique. They embedded multiple copies of the same information in several bits of the cover image starting from the lower order to the higher orders. So even if some of the information is lost due to an attack, they still collect the remaining information and recover the watermark from the cover image using the bit majority algorithm.

Xiang-Gen Xia et al. [16] proposed a watermarking technique based on the Discrete Wavelet Transform (DWT). They perform two-level decomposition using the Haar wavelet filters. The watermark, modeled as Gaussian noise, was added to the middle and high-frequency bands of the DWT transformed image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images.

III. PROBLEM STATEMENT

Block histogram shifting (BHS) is the blocking effect and block histogram shifting method low robustness. The problem with these blocks is that when the image is less robustness to low PSNR ratios, these blocks become visible and data hiding not proper. This has been termed as the blocking effect. The goal of the research is to data hiding proper the source image using a histogram shifting algorithm and color the reconstructed into a gray image obtained good robustness and optimal solution.

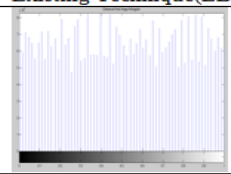
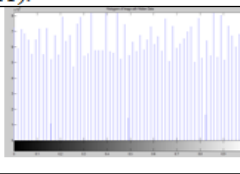
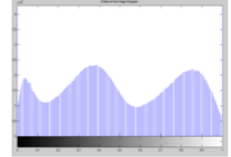
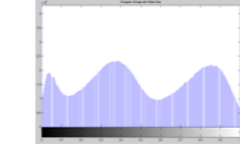
III. MATLAB TOOL

Compare the proposed mechanisms with the existing algorithm. The experiment is performed on a laptop with an Intel Dual Core processor (1,836 Hz), 2 GB of memory and Windows 7 final system. Here, this method is applied and simulated in MATLAB 7.8.0 and for this work, we use the Intel machine 1.4 GHz with the operating system Windows 7, Windows-x, etc. The performance analysis of the MATLAB version (R2008a) which is, used for this thesis Mining provides libraries optimized for processors for rapid execution and computation and is performed in Data Cancer Data. It uses its JIT compilation technology (just in time) to provide execution speeds that rival traditional programming languages. It can also be an additional advantage of multi-core computers and multiprocessors; MATLAB provides many alerts and multi-process numerical functions. These functions automatically run on multiple computer threads during a single MATLAB, running faster on multi-course computers. During this thesis, all improved results of effective data recovery were performed in MATLAB (R2008b). It is the high-level language and interactive background used by many universal engineers and scientists. It allows exploring and visualizing ideas and working together in different disciplines and process signals and images, messages and calculations of results

IV. RESULT ANALYSIS

In a study in the field of the watermark could also be of a visible or invisible kind and every methodology has its own strengths and weaknesses. The standard of watermarked pictures is measured in terms of MSE and PSNR (Peak Signal to Noise Ratio) and notice is a reliable image, authentication, information hiding, and sensible hardness. Proposed technique an improved robust image encryption histogram shifting method based on bits changing using data hiding in encrypted image based on bit changing in the histogram and proposed method a is robustness is high-quality as compare existing method block histogram shifting (BHS). Experimentation1 Base on Male whitetail deer and Vodafone logo: Experimentation1 base on male whitetail deer and Vodafone logo images like Male whitetail deer (in jpg 89.3KB) host image and dimension 512x512. Vodafone logo as data image (in jpg size 6.91KB) and dimension 304x166. Male whitetail deer image as a host image and Vodafone logo image as data image both are embedding using existing technique (EBHT) and generate data hiding image histogram. Male whitetail deer image as a host image and Vodafone logo image as data image both are embedding using new technique (SRDHHT) and generate data hiding image histogram.

Table1Result Analysis between Existing Method and New Method

Existing Technique(EBHT):	
	
MSE	0.0050625
PSNR	54.114
New Technique (SRDHHT):	
	
MSE	0.0042217
PSNR	55.931

Comparison graph between existing technique (EBHT) and new technique (SRDHHT) shows result graph and find existing technique (EBHT) low PSNR and high MSE other new technique (SRDHHT) high PSNR and low MSE.

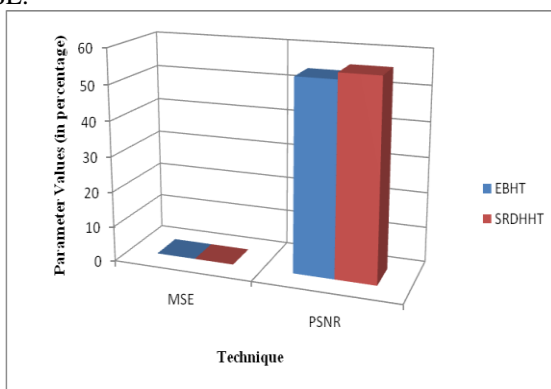


Fig3 Experimentation1 Base on PSNR and MSE

V CONCLUSION

Secure reversible data hiding histogram technique (SRDHHT).Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which is proposed by reserving room before encryption. Data hiding schemes for an encrypted image with a low computation complexity is analyzed, which consists of image encryption, image data hiding, and image data extraction and image recovery phases. The original images data are encrypted by a new encryption approach. Image encryption strategy is performed and although a data hider does not know the original content, embeds the secret image data increases noisy in block histogram shift technique, the smaller the block size, low embedding capacity. Our proposed are not affected by noise and bit histogram shift is performed without blocks effect. They consider block-based watermarking are more MSE and less PSNR values. They additionally study on some papers of image watermarking. Different techniques of digital image data hiding supported spatial and frequency domain techniques are mentioned. Our Proposed technique (SRDHHT) can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy, this novel method can achieve real reversibility; separate data extraction and great improvement on the quality of marked decrypted images secure reversible data hiding histogram technique. The experimental results show that the proposed technique histogram specification is better PSNR and less MSE than the existing technique.

Reference

- [1]. Manpreet Kaur, Sonika Jindal, Sunny Behal “A Study of Digital Image Watermarking” IJREAS Volume 2, Issue 2, ISSN: 2249-3905, pp. 126-136, February 2012.
- [2]. Zhu Xiaosong, Mao Yaowu, Dai Yaowei, Wang Zhiquan, “HVSbased wavelet watermarking scheme “Journal of Nanjing University of Science and Technology, Vol.25 No.3:262-268, Jun.2001.
- [3]. Usha Pal, Dinesh Chandra, “SURVEY OF DIGITAL WATERMARKING USING DCT”, International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397 Vol. 4 No. 09 Sep 2012.
- [4]. F. A. P. Petitcolas, R.J. Anderson, R. J., and M. G. Kuhn, “Information hiding - A survey,” Proceedings of the IEEE, Volume 87, Issue 7, 1999, pages 1062-1078.
- [5]. M. L. M. Ingemar J. Cox, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, Digital Watermarking and Steganography: Morgan Kaufmann Publishers, 2008.
- [6]. N. Cvejic, "Algorithms for Audio Watermarking and Steganography," Department of Electrical and Information Engineering, University of Oulu, 2004
- [7]. S. Jun and M. S. Alam, "Fragility and Robustness of Binary Phase-Only-Filter-Based Fragile/Semi fragile Digital Image Watermarking," Instrumentation and Measurement, IEEE Transactions on, vol. 57, pp. 595-606, 2008.
- [8]. L. Jian and H. Xiangjian, "A Review Study on Digital Watermarking," in Information and

- Communication Technologies, 2005. ICICT, 2005. First International Conference on, 2005, pp. 337-341.
- [9]. C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," *Proceedings of the IEEE*, vol. 90, pp. 64-77, 2002.
- [10]. R. F. Olanrewaju, "Development of Intelligent Digital Watermarking via Safe Region," Ph.D., Electrical, and Computer Engineering, International Islamic University Malaysia, Kulliyah of Engineering, 2011.
- [11]. W. H. Cho, M. E. Lee, H. Lim, and S. Y. Park, "Watermarking technique for authentication of 3-D polygonal meshes," in *Proc. of the International Workshop on Digital Watermarking'05*, 2005, pp. 259-270.
- [12]. Mohamed Ali HAJJAJI Abdellatif MTIBAA El-bey Bourenane, "A Watermarking of Medical Image: Method Based "LSB", *Journal of Emerging Trends in Computing and Information Sciences*, VOL. 2, NO. 12, December 2011, ISSN 2079-8407, pp. 714-721.
- [13]. E. Praun, H. Hoppe, and A. Finkelstein, "Robust mesh watermarking," in *Proc. of the ACM SIGGRAPH Conference on Computer Graphics'99*, 1999, pp. 49-56.
- [14]. Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, Senior Member IEEE, "A Dual Digital-Image Watermarking Technique" *World Academy of Science, Engineering and Technology* 5 2005, pp. 136-139.
- [15]. Manjit Thapa, Dr. Sandeep Kumar Sood, and A.P Meenakshi Sharma, "Digital Image Watermarking Technique Based on Different Attacks", *International Journal of Advanced Computer Science and Applications*, Vol. 2, No. 4, 2011.
- [16]. Xiang-Gen Xia, Charles G. Poncelet, and Gonzalo R. Arce, "A Multiresolution Watermark for Digital Images" *Proc. IEEE Int. Conf. on Image Processing*, Oct. 1997, vol. I, pp. 548-551.
- [17]. X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826-832, Apr. 2012.
- [18]. C. Anuradha and S. Lavanya "A secure and authenticated reversible Data hiding in encrypted images", *IJARCSSE*, 2013.
- [19]. Subhanya R.J (1), Anjani Dayanandh N (2)"Difference Expansion Reversible Image Watermarking Schemes Using Integer Wavelet Transform Based Approach". *International Journal of Engineering Research and Applications (IJERA)* ISSN: 2248-9622 International Conference on Humming Bird (01st March 2014).
- [20]. Hamid, Nagham, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qureshi. "Image steganography techniques: an overview." *International Journal of Computer Science and Security (IJCSS)* 6, no. 3: 168-187, 2012.
- [21]. Rao, Raghuvver M., and Manoj K. Arora. "Overview of image processing." *Advanced image processing techniques for remotely sensed hyperspectral data*, pp. 51-85. Springer, Berlin, Heidelberg, 2004.