Shweta Singh et al. 2019, 7:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

A Survey on Various Techniques and Features of Digital Image Data Watermarking

Shweta Singh
Dept. of Computer Science & Engg.
IES College of Technology
Bhopal, MP, India

Abstract

As the computerized world is developing with different sort of information like content record, picture, video. Out of those picture assumes a significant job in various field, for example, remote detecting, internet based life, and so on. So keep up the picture quality is finished by Digital image processing on different issues. This paper gives a concise study of image proprietorship maintenance by information concealing procedures for different type of images. Picture investigation features are portray in this paper with their fundamentals. As watermark information is invisible yet it has to maintain some properties of watermarking which are likewise explain in this paper as they are the best measure for comparing various procedures of watermarking work. Detail discussion of various researcher works was also brief in this paper.

Keywords: Digital Image Processing, DCT, Information Extraction, LSB, Watermarking.

I. INTRODUCTION

As internet, for the various parts, could be a user friendly place wherever individuals have an interest in downloading photos, music, and videos. The web provides an encrypted economical delivery system that's comparatively cheap. Exploit various media via the web needs a fraction of the time to a physical store to buy said media. Also, when one purchases media over the web, one solely would like virtual house to store the media in question as against storing it on a shelf or where such media may well be placed. On the other hand, such availability provides folks with the likelihood of copyright violations.

The technology that media owners applied to safeguard their content is cryptography. Since cryptography was used, this can be the foremost common methodology for defense and the most developed. The gathering of files would be encrypted by utilizing an encryption key. The files Would then be dispersed to paying customers. At last, the client would use a decryption key, provided by the distributer, to access the set of files. The chance of somebody exploit the set of encrypted In different words, whereas cryptography will shield files from interception, the technology won't shield files from the tip user.So to defeat these completely different techniques are use for protecting the proprietary of the owner. One of such digital approach is watermarking that could be a subdivision of concealing information that's accustomed place some information within the original image which can specify the originality of the digital knowledge like pictures, digital music, or digital video [1, 2, 4]. One of the essential reasons for the copyright issue is that the ease offered of the web and a few codes which will modify the content as per the user demand.

Watermark is generally divide into two classes first is visible watermarking and other is invisible watermarking. Here watermark information seen by naked eyes is taken into account as visible watermarking as shown in fig. 1.Where in case of invisible watermark data isn't visible by naked eyes as shown in fig. 2, though watermark data is hidden within the original data. Data could also be of any digital information like document, image, video file,

etc.

Figure 1: Visible watermark in image data.

Figure 2: Visible watermark in image data.

Rest of this paper was organized into few sections. Second section shows many properties of watermarking. Next section shows connected work section provides a summary of many different author technique adopted by scientist for embedding and extraction of watermark. Next section provides an assortment of various visual options of the image. Finally whole work was finished with future work.

II. PROPERTIES OF WATERMARKING

A successful watermarking system should have the following characteristics:

1. **Imperceptibility:** In language of watermarking, physical property means after adding the watermark information, wrap medium should not modify much. In different words it's not desired that projected watermarking rule can have an effect on the image quality. Thus those rule that don't satisfy this condition got to face knowledge owner acceptableness because it scale back the image or carrier signal originality that isn't required by utilizing this method.
2. **Robustness:** During this watermarking algorithm bear the responsibility that by applying traditional manipulation operation it shouldn't have an effect on the image quality. Thus this can be desired property of watermarking that depends on the embedding method and space wherever watermarking is embedded.
3. **Fragility:** During this property watermarking data could get modified by applying some malicious operation. Thus these operations alter the embedded knowledge that isn't desired So some temper recognition measure need to be present at receiver end for the detection of fragile attack. The semi-fragile watermarking includes a fragile watermarking part and a strong watermarking part i.e. semi-fragile watermarking are strong to some attacks however fragile to others attacks.
4. **Resilient against signal processing:** During this property watermarking rule algorithm need to be protective against common signal processing algorithms like digital to analog conversion or analog to digital conversion. Re-sampling, re-quantization that involve video digitizing still as recompression. In a number of transmission operation like filtering of information by passing this from low or high pass filter, compression for low house, conversion of information from one format to different like if in case of image JPEG, BMP, GRAY, HSV, etc.
5. **Resilient to common geometric distortions (image and video data):** Watermarking in image and video data ought to even be immune from geometric image operations like rotation, translation, cropping and scaling. This material isn't necessary for audio watermarking.
6. **Robust against forgery and collusion:** Here watermarking rule ought to be protecting against some conspiracy attack. Several people, who have a watermarking photocopy copy of the data, would possibly conspire their watermarking copies to end the watermarking being there and will manufacture a replica of the main copy. In advance, if a digital watermarking is to be utilizing in court case, it got to be not going for colluders to link their image to form a dissimilar appropriate watermarking.

7. **Unambiguousness**: Recovery of the watermarking is meant to unambiguously acknowledge the owner. In addition, the correctness of owner recognition shouldn't corrupt a lot of within the case of an interloper attack. In [7] have exposed extraordinary accomplishment in removing knowledge embedded by commercially procurable algorithms.

III. RELATED WORK

Mohammed A. M. Abdullah et. al. in [11] has projected a watermarking technique by inserting binary data in DCT middle band frequency region. During this paper image was blocked into fix size while per watermark bit DCT middle band fix co-ordinates values were swapped. Swapping of this was rely upon bound conditions, thus same set of conditions were maintained at receiver aspect for watermark extraction. This work faces low watermark absorption with low struggle against abstraction attacks.

Kazuki Yamato et al. in [12] has projected a between category variance construct for inserting image in edge region of the image. Author has first applied discriminate analysis methodology for changing image into binary format, than apply BCV technique that classify element into edge and non-edge region. Modification in abstraction region of the image was in dire straits concealing knowledge into image edge region. Here low house offered for watermark whereas embedding in edge region is simple to trace the secret information.

Angela Piper et al. in [13] generate watermark from the input image solely and plant in low waveband of image. During this paper fragile watermarking technique was projected that preserve pictures against JPEG compression attack. Here paper has not cover different kind of attack, whereas execution time of this work was additionally quit high.

Hanieh Khalilian et al. [14], projected a fractal code primarily based self reconstruction algorithm wherever input image was send extremely noisy area. Thus loss of knowledge was assumed that was recovered by further packets of fractal code. Tempering of image was additionally preserved to by hashing hash key as secret information. This paper has improved the strength in losy surroundings however it needed further information measure with process complexness.

In [15] author has projected a Singular worth Decomposition technique to search out match knowledge within the original image. Authors of this paper divide image into fix size patch and swap those patch with KSVD patch. This increases the image security in network whereas encryption of watermark was additionally done before embedding. Here looking out of correct patch from KSVD library was time taken. Dictionary storage at sender or receiver aspect was additionally large. In CNN was used for embedding the watermark data in original image. With the assistance of some supporting information it absolutely was found that Watermarking was extract from the image. Here it absolutely was obtained that both Watermarking and image got reverse at the receiving finish.

Huang et al. [16] have projected a unique blind watermarking technique using Back Propagation neural network in riffle domain. During this paper, a disorganized watermark is embedded using the advantage of Human Vision System (HVS) to attain higher physical property and strength. Neural network is employed to con the relation between the embedded watermark and corresponding watermarked image.

Peng et al. [17] have projected a unique image watermarking technique in multi-wavelet domain supported SVM. The algorithm has used special waveband and also the property of image for watermarking. Though the scheme is logically robust against various however fails to attain strength against average filtering, median filtering, JPEG attacks and scaling attack successfully.

Yang et al. [18] have additionally projected a powerful technique in undecimated discrete wavelet transform (UDWT) domain using fuzzy SVM for geometric twist correction. Although the technique provides adequate strength, nonetheless it needs excessive process time and additionally it's not strong to native geometric distortions.

In [19] third level LFT (Lifting Fourier transform) as used for inserting watermark. Trait set produced from the blocks during which reference watermark RW was embedded has been utilised as input feature vector in Feed Forward neural network. The corresponding bits of RW are used as aim vector.The technique provides satisfactory strength against

completely different attacks like noising attacks, de-noising attacks, some geometric attacks, etc.

1.Features for Data hiding

As Image is assortment or sequence of element and every element is treat as single worth that could be a quite cell during matrices. So as to spot an object in this image some options got to be maintained as different object have different feature to spot them that are elaborated below:

2. Colour feature- Image could be a matrix of light strength values, these intensity values represent completely different type of colour. Thus to spot an object colure is a very important feature, one vital property of this feature is low computation price.

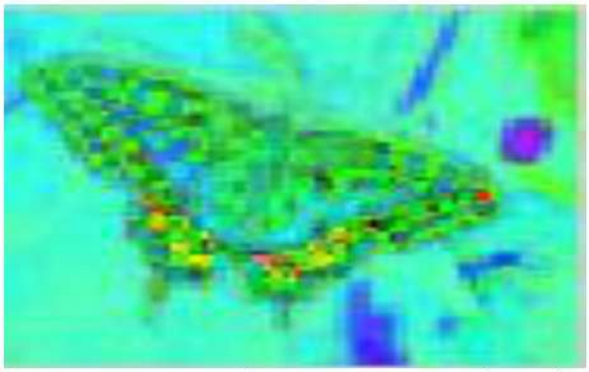

Figure 3: Represent the HSV (Hue Saturation value) format of an image.

Different Image files available in different color formats like images have different colure format ranging from RGB that indicate red, green, and blue. This can be a three dimensional illustration of one image during which two dimensional matrix represent single color and assortment of these matrix tends to third dimension. So as to form intensity calculation for every element grey format is use that could be a two dimension values vary from zero to 255. If in case of binary format that could be a black and white colour matrix whose values area unit solely zero or one. With the assistance of this colour feature face has been detected expeditiously in [8].

3. Edge Feature- As image could be an assortment of intensity values, and with the fast modification within the values of a picture one vital feature arises because the Edge as shown in figure 4. This feature is use for various kind of image object detection like building on a scene, roads, etc [7]. There are several rule has been developed to effectively illustrate all the pictures of the image or frames that are Sobel, perwitt, canny, etc. out of those algorithm canny edge detection is one amongst the most effective algorithm to search out all potential boundaries of a pictures.

Figure 4: Represent Edge feature of an image.

4.Texture Feature: Texture could be a degree of intensity distinction of a surface that enumerates properties like regularity and smoothness [6]. Compared to paint house model, texture needs a process step. The feel options on the premise of color are less sensitive to illumination changes as same on edge options.

5. Corner Feature: So as to stabilize the video frames in case of moving camera it need the distinction between the two frames that are illustrated by the corner feature within the image or frame. Thus by finding the corner position of the two frames one can notice resize the window in original read. This feature is additionally use to search out the angles still because the distance between the item of the two completely different frames. As they represent purpose within the image thus its use to trace the target objects.

Figure 5: Represent the corner feature of an image with green point.

V. WATERMARK ATTACKS

As video shift from one place to a different by a network. Thus movement of video build varied changes within the original data. thus it's needed that data hiding or data hiding technique ought to be powerful against varied attacks that is describe in following points.

1. Noise Attack: This can be quite common drawback within the transfer channel where the information is send in the data consist of some other information. Thus merging with different data cause small change in the data that is term as noise within the original signal. In experiment completely different noise manufacturing feature is used for adding these noise within the data like : Gaussian Noise Attack, Salt & Pepper Noise, Speckle Noise Attack, etc.

2. Filter Attack: During this kind of attack a completely different servers act because the intercessor for passing the information from sender to receiver end thus filter use in those server build few changes within the data. This can be term as filter attack. In experiment same kind of attack is completed by applying the filters like average filter, motion filter, sharpen filter, etc [6,7].

3. Compression Attack: In different case once data is compress for Various demand information hide within the video get loss. Thus algorithm ought to be protecting against such kind of compression attacks. Some time due to change in video format different compression algorithm use different frame compression technique [7]. Some filtering attacks are: MP4compression, MPEG compression, etc.

4. Scene Swapping: This can be count as temporal attack where video frame are swap with its own frame. During this kind of attack connection between the watermark extraction get loss and extracted frame get extremely affected so data hiding algorithm that was relying upon frame sequence isn't robust against this attack.

VI. CONCLUSIONS

In today's world security of the image is very important. This paper has surveyed different problems and techniques proposed by researcher for invisible watermarking. As conclude that all techniques are good for image watermarking and have their own advantages, disadvantages. It has been observed that during extraction watermark is the main focus of most of the researcher but few of them work on original image as well but reverse process of both watermark and original image is still not done. Watermark is mainly compare on the basis of the attack but most of the paper work on the spatial attack and show effective results in various attacks with different levels. A special calculation is still required which protect both watermark and carrier image with high strength against geometric, spatial types of attacks.

REFERENCES

[1]. Tamanna Tabassum, S.M. Mohidul Islam "A Digital Image Data Hiding Technique Based On Identical Frame Extraction In 3-Level DWT" Vol. 13, No. 7, Pp. 560 –576, July 2003.

[2]. Frank Hartung, Jonathan K. Su, And Bernd Girod "Spread Spectrum Data Hiding: Malicious Attacks And Counterattacks". Of Multimedia Contents" International Journal Of Research In Engineering And Technology Eissn: 2319-1163 | Pissn: 2321-7308, 2005.

[3]. Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ And Shigeo Kato . "Digital Image Data Hiding Method Using Between-Class Variance". 978-1-4673-2533-2/12/$26.00 ©2012 IEEE.

[4]. Angela Piper1, Reihaneh Safavi-Naini. "Scalable Fragile Data Hiding For Image Authentication". Published In IET Information Security, On 31st December 2012

[5]. Reema Rhine, Nikhila T Bhuvan. "Image Scrambling Methods for Image Hiding: A Survey". IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.2, February 2015

[6]. MohammadReza Keyvanpour*a, Farnoosh Merrikh-Bayatb. "An Effective chaos-based image watermarking scheme using fractal". Science Direct, Procedia Computer Science 3 (2011) 89–95.

[7]. Yicheng Sun, Xiubao Sui, Guohua Gu, Yuan Liu, Shuangshuang Xu. "Compressive Super-Resolution Imaging Based on Scrambled Block Hadamard Ensemble". IEEE Photonic Journal, Volume 8, Number 2, April 2016, 1943-0655.

[8]. Hanieh Khalilian, Student Member, IEEE, and Ivan V. Bajic Video "Watermarking With Empirical PCA-Based Decoding" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 12, DECEMBER 2013.

[9]. Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, And Xiaojie Guo. "High Capacity Reversible Watermarking In Encrypted Images By Patch-Level Sparse Representation". IEEE TRANSACTIONS ON CYBERNETICS 2015.

[10]. Qingtang Su, Decheng Liu, Zihan Yuan, Gang Wang, Xiaofeng Zhang, Beijing Chen, And Tao Yao. "New Rapid And Robust Color Image Watermarking Technique In Spatial Domain". Ieee Access March 25, 2019.

[11]. Pawe Korus, Student Member, Ieee, And Andrzej Dziech. "Efficient Method For Content Reconstructionwith Self-Embedding". Ieee Transactions On Image Processing, Vol. 22, No. 3, March 2013.

[12]. L. M. Vargas And E. Vera, "An Implementation Of Reversible Data Hiding For Still Images" Ieee Latin America Transactions, Vol. 11, No. 1, Feb. 2013.

[13]. Angela Piper1, Reihaneh Safavi-Naini. "Scalable Fragile Data Hiding For Image Authentication". Iet Inf. Secur., 2013, Vol. 7, Iss. 4, Pp. 300–311

[14]. Ioan-Catalin Dragoi, Member, Ieee, And Dinu Coltuc . "Local-Prediction-Based Difference Expansion Reversible Data Hiding" . Ieee Transactions On Image Processing, Vol. 23, No. 4, April 2014.

[15]. Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, And Xiaojie Guo. "High Capacity Reversible Data Hiding In Encrypted Images By Patch-Level Sparse Representation". Ieee Transactions On Cybernetics 2015.

[16]. A.F.Elgamal, N.A.Mosa , W.K.Elsaid A Fragile Video Data Hiding Algorithm For Content Authentication Based On Block Mean And Modulation Factor International Journal Of Computer Applications (0975 – 8887) Volume 80 – No.4, October 2013.

[17]. Nallagarla.Ramamurthy#1 And Dr.S.Varadarajan. "Effect Of Various Attacks On Watermarked Images. "International Journal Of Computer Science And Information Technologies, Vol. 3 (2) , 2012,3582-3587

[18]. Priya Porwal1, Tanvi Ghag2, Nikita Poddar3, Ankita Tawde Digital Video Data Hiding Using Modified Lsb And Dct Technique. International Journal Of Research In Engineering And Technology Eissn: 2319-1163.

[19]. Mr Mohan A Chimanna 1,Prof.S.R.Kho "Digital Video Data Hiding Techniques For Secure Multimedia Creation And Delivery" Vol. 3, Issue 2, March -April 2013, Pp.839-844839.