A Survey on Digital Image Watermarking

Rohit C Sukhasare[1], Suresh C Kuri[2]
[1,2]KLS's Gogte Institute of Technology, Belagavi, India

Abstract— Advanced image watermarking might be a marginal investigation space and it plays a significant half in information security. From the review of the precision and fundamental choices of watermarking the structure of watermarking is given. The structure has 2 components that are watermark addition, discovery and extraction. In view of the importance of digital images copyright protection, based on the analysis of the main digital watermarking algorithms, the digital watermarking technology can be applied to the image copyright protection. Recently, computerized information is regularly just controlled, replicated, dispersed and stored, that has come about inside the interest for safe ownership of the information. The ideas of watermarking and their traits, assaults, embedding and extraction technique. At last, the present work in this field are discussed in this paper.

Keywords: Digital Watermarking, CNN, DCT, attacks, SVM.

I. INTRODUCTION

The advanced media like picture, sound and video zone unit a significant method for communication within the world and being more and more used for delivery of transmission content, so it's simple to govern, store, distribute or reproduce the info. This shows there's no distinction within the quality of derived and original pictures. However, unconditional repetition will cause monetary losses and issues for material possession rights [3].data concealment technique is used to watch pictures in this manner watermarking has transformed into a noteworthy examination space. Progressed watermarking modules are proposed to make prosperity, affirmation and copyright security of the substance [4]. amid this procedure we will in general guard the host picture from felonious addition of solid complete. The watermarking algorithms should be undetectable to the optic, durable against attacks, blind which implies the initial image isn't necessary for the detection and extraction of the complete. The important choices of computerized watermarks region unit strength, physical property, limit, security and procedure cost. Machine learning could be a technique to see predict from its past behaviours and learning. It is a way that improves the detection rate of watermarks once being attacked and contains varied ways for various classification and patterns for recognition of downside time overwhelming activity with automatic techniques used for improvement of accuracy and potency. Generally, four varieties of attacks on digital watermarking systems are as mentioned:

A. Active attacks: In active attacks hackers tries to get rid of watermark. They are geared towards noise of watermark before recognition. This shows that the matter in copyright protection, copy management, etc.
B. Passive attacks: In passive attacks, hackers simply tried to work out that there is watermark and determine it. During this attack no harm or removal is completed.
C. Forgery attacks: During this attack the hacker will simply manipulate the information and makes corrupted image real.
D. Collusion attacks: In this attack the hackers have identical import as for the actives ones however used slightly totally different approach. The hacker uses instances of same information to construct the new copy while not watermark.

In general, watermarking system consists of two processes, embedding and extraction. The embedding process is consisting of encoding [8]. It is used to produce the watermarked image. The watermark embedding process takes a cover image (C), watermark image (WI) and secret key (K) then it goes to embedded function gives watermarked image (WE). The extraction process is consisting of recovery process. It is used to recover the corrupted image, which may or may not be the watermarked image. The extraction process takes cover image and watermarked with secret key to recover the watermark from the possibly distorted image [9-10]. The watermark embedding and extraction process is given in Figure 1(a) and Figure 1(b) respectively. The watermark embedding process can be written as:

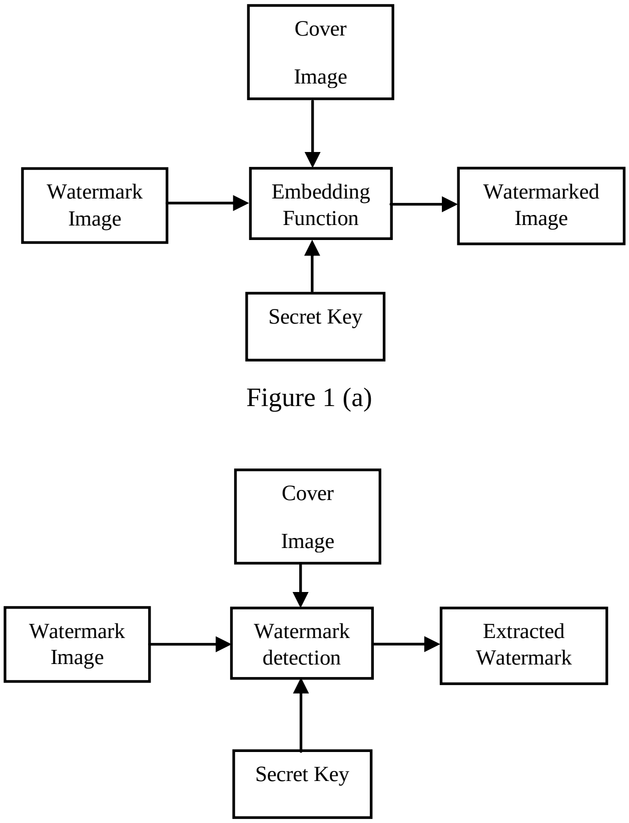

Figure 1 (a)

Figure 1 (b)

Figure 1: Watermark (a) Embedding process and (b) Extraction process

II. RELATED RESEARCH WORK

Sheng [1] proposed a strategy amid which the watermark is implanted and separated through explicit FCNN (Full Counter-engendering Neural System) for computerized watermarking, very surprising from the ordinary ways, the different spread pictures and in this manner the watermark are implanted inside the neurotransmitters of a FCNN in the meantime instead of the cover pictures. Therefore, the watermarked image is sort of the same the original image. Furthermore, the greater part of the assaults couldn't debase the standard of the extricated watermark picture. The experimental results show that the proposed technique is ready to realize lustiness, imperceptibility and credibleness in watermarking.

Ri Piao et al. [2] proposed a replacement Human sensory system (HVS) model primarily based blind watermarking theme during which a watermark is embedded into the discrete wavelet transform (DWT) space. This system utilizes the HVS model and Radial Basis Function Neural Network (RBFNN). They use RBFNN to enter and extract the watermark. They more use the involve Artificial Neural Networks having HVS characteristics to work out the insertion strength of the random sequence watermark. A mystery key's acclimated confirm the begin position of the picture wherever the watermark is to be inserted. The authors claim that this method prevents pirates from removing the watermark simply. Their trial results demonstrate that their strategy has shrewd physical property and high vigour to the regular picture process assaults. They report that they need obtained a PSNR value larger than forty-five dB just in case of all pictures. They claim that because of adjustive capabilities of the RBF network, the embedding / extraction strategy will usually improve robustness against the chosen image process attacks they are doing not work out the time interval spans of RBF network training, embedding and extraction.

Mishra et al. [5] have as of late proposed a one of a kind computerized picture watermarking algorithmic based on Extreme Learning Machine (ELM) for 2 grey scale pictures. As mentioned, the ELM algorithmic program is extremely quick and completes its coaching in milliseconds not like its different counterparts like BPN or Fuzzy illation System (FIS). During this paper, they report that their algorithmic program trains the ELM by exploitation low frequency coefficients of the grayscale host image in transform domain. The prepared ELM creates a succession of 1024 genuine numbers, standardized predictable with N (0, 1) as partner yield. They utilize this arrangement on the grounds that the watermark to be implanted among the host picture misuse Cox's recipe [15] to get the marked picture. The visual quality of the signed pictures is quantified by PSNR. The authors report high PSNR values that indicate that the standard of signed pictures is nice. The computed high price of SIM (X, X*) establishes that the extraction method is in and consistent with authors, the algorithmic program finds smart sensible applications, particularly in things that warrant meeting time constraints, this can be because of, they get the instructing time.

Huang et al. [6] built up a totally interesting visually impaired watermarking system upheld Back Spread Neural System inside the wavelet domain. As per this scheme, with the employment of HVS characteristics, a disorganized watermark is observably embedded in a very sturdy manner. A neural network is with success want to memorise the relation between the watermark and also the corresponding watermarked image. This way, the authors are productive to blindly recover the precise watermark from the signed image. Their results indicate that the planned scheme offers sensible physical property and high strength to varied image process attacks.

Shwu-Huey Yen and Chia-Jen [7] Wang proposed an advanced watermarking strategy upheld Support Vector Machines (SVMs). Use the good characteristic of the SVM, which might result associate degree optimum hyperplane for the given training samples, the physical property and hardiness needs of watermarks area unit consummated and optimized. Inside the anticipated topic, to help physical property, the watermark is inserted by unsymmetrically tuning blue channels of the focal and close pixels at constant time. in addition, to push strength, the implanted watermark bits will be re-altered if fundamental with regards to grouping aftereffects of the prepared SVM. Their theme uses solely 128 bits in coaching SVM, therefore it's time economical. Watermarks zone unit embedded in spatial space and separated straightforwardly from a watermarked picture while not the need of unique picture. Tests demonstrate that the anticipated topic gives high PSNR of a watermarked pictures and low extraction error rate.

Bibi Isac and V. Santhi [8] proposed an in-depth description of watermarking works applied victimisation digital pictures and videos supported neural networks is given. several of those techniques are able to satisfy the essential demand of watermarking i.e. the extraction method doesn't need the first signal or in different words, the rule is blind. equally in few papers it's found that employment is applied in special domain, whereas others work square measure applied in frequency domain by victimisation transformation techniques. The neural systems that square measure utilized grasp Back spread Network (BPN), Counter Propagation Network (CPN), Full Counter Propagation System and Cell Neural Network (CNN). The strength of those algorithms square measure tested with relevance varied attacks like blurring, median filtering attack, low-pass filtering attack, cropping assault and salt and pepper clamour assault. Thus, a perfect watermarking rule ought to be blind in nature and should be sturdy against attacks. Additionally, it must guarantee correct and quick watermark detection with low error rate.

Aidin Ferdowsi and Walid Saad [9] proposed a totally remarkable profound learning procedure for dynamic watermarking of IoT signs to locate digital assaults. The planned learning framework, supported anlong short-term memory (LSTM) structure, permits the IoT devices to extract a collection of random options from their generated signal and dynamically watermark these options into the signal. This technique permits the IoT's cloud centre, that collects signals from the IoT devices, to effectively manifest the dependability of the signals. what is more, the planned technique prevents difficult attack situations like eavesdropping within which the cyber assailant collects the info from the IoT devices and aims to interrupt the watermarking formula.

Xiaoyi Chou et al. [10] proposed associate degree improved theme to extend the lustiness of embedded data on the idea of discrete cosine transform (DCT) domain. Directly off the bat, the introducing power with support vector machines (SVMs) was adaptively strong by training 1600 picture deters that square extent of various surface and radiance. Besides, the installing position with the advanced hereditary equation (GA) was picked. To optimize GA, the simplest individual within the 1st place of every generation directly went into successive generation, and therefore the best individual within the second position participated within the crossover and the mutation method. The transparency reaches forty.5 once GA's generation variety is two hundred. A contextual analysis was directed on a 256 × 256 standard Lena pictures with the arranged philosophy. When changed assaults, (for example, trimming, JPEG pressure, mathematician low-pass sifting (3, 0.5), histogram equalization, and qualification expanding (0.5, 0.6)) on the watermarked picture, the isolated watermark was differentiated and the first. Results demonstrate that the watermark are often effectively recovered once these strikes. Although the formula is weak against rotation attacks, it provides top quality in physical property and robustness and thus it's a productive contender for implementing novel picture watermarking topic meeting genuine courses of events.

Nazir A. et al. [11] presented a disorderly encryption-based visually impaired computerized picture watermarking method appropriate to each grayscale and shading pictures. Unmistakable Discrete cosine transform (DCT) is utilized before implanting the watermark inside the host picture. The host image is split into eight nine eight nonoverlapping blocks before DCT application, and therefore the watermark bit is embedded by modifying distinction between DCT coefficients of adjacent blocks. Arnold transform is employed additionally to chaotic cryptography to feature double-layer security to the watermark. Three totally various variations of the anticipated algorithmic program are tried and dissected. The re-enactment results show that the foreseen subject is strong to by far most of the image technique assignments like joint picture capable gathering weight, sharpening, cutting, and centre fixing. To validate the potency of the projected technique, the simulation results square measure compared with bound state-of-art techniques. The comparison results illustrate that the projected scheme performs higher in terms of strength, security, and imperceptivity. Given the merits of the anticipated subject, it will be utilized in applications like e-medicinal services and telemedicine to powerfully stow away electronic wellbeing records in restorative pictures.

Vatsa et al. [12] proposed biometric primarily based image watermarking formula wherever face image is embedded within the fingerprint. The embedding watermarking technique supported Discrete Wavelet Transform (DWT) and Support Vector Machine (SVM). The experimental results shown that the tactic is powerful and therefore the face image is resilient to geometric and frequency attacks. the blend of SVM improved the face acknowledgment by 100 percent.

Jianzhen et al. [13] anticipated an RST (Rotation, Scaling and translation) invariant watermarking method using SVM and picture minutes for synchronization. In watermarking strategy to gauge RST improve parameters SVM is utilized to discover the picture geometric example outline by six consolidated low request picture minutes. The exploratory outcome demonstrates that subject will oppose JPEG pressure, noise and geometric assaults.

Lei Li et al. [14], proposed a picture watermarking plan utilizing spatial space dependent on Fussy Support Vector Machine (FSVM). In the inserting procedure, the 8 * 8 square of the spread picture is partitioned into sub-square of the surface highlights as info vectors utilizing support vector machine. The picture sub square is separated into a feeble surface and a solid surface. The solid surface data is implanted into the spread picture. The technique has been demonstrated that the heartiness of the FSVM based strategy is superior to SVM based technique against significant assaults.

Jain et al. [15], anticipated a watermarking algorithmic standard bolstered bolster vector machine exploitation shading picture. Within the embedding method, the watermark is embedded into the distinct ripple domain of the initial image and extracted by coaching support vector machine. moreover, the methodology is exploitation energy consistent to downsize the blunder and increment the speed of the instructive. The trial results are demonstrated that the strategy is imperceptible against flag process assaults. However, the worth of PSNR is below than twenty-seven decibel for many of the attacks.

Vafaei et al. [16] proposed a strong blind watermarking technique. The watermarking technique uses the Neural Networks in Discrete Wavelet Transform domain. The neural systems association strategy is utilized to develop the idea of watermark picture. The test outcome exhibits that technique is strong and in cognoscible to different strikes.

Yahya et al. [17] arranged a model for information security misuse stego SVM characterization. The embedding technique uses LSB in image steganography that hides information behind a cover-image during spatial and discrete cosine transform (DCT) domain. The technique planned a brand-new model that utilizes Human sensory system (HVS) and embedding technique through shifted LSB referred to as Stego SVM- Shifted LSB in DCT space to spare the physical property and addition the nature of stego-pictures.

Zand and Li [18] proposed a completely unique watermarking formula for non-compressed video wherever, the initial video frame is split into 8×8 blocks. DCT (Discrete Cosine Transform) was applied on these 8×8 blocks to calculate the energy from the DCT coefficients. consistent with the energy calculated, the areas within the blocks were classified information contained and motion. The watermark embedding space was determined. Within the watermark extraction a BPN (Back Propagation Network) was trained so as to observe the areas wherever the watermark is embedded supported the DCT constant energy values.

III. OBSERVATION

A comprehensive set of papers which are published in this direction have been studied. It is concluded that although the BPN based watermarking techniques are able to optimize the visual quality and robustness of the embedding scheme, yet it consumes a large time span to finish various processes involved. The Radial basis Function based network is capable to resolve the problem encountered by the BPN based schemes. It is generally implemented in the DWT domain and therefore gives better results in terms of the visual quality of signed images as compared to DCT – BPN based approach. Hybrid approaches are also found suitable for this purpose. GA-BPN based watermarking scheme is quite suitable as the visual quality and robustness issue is optimized by using it. The time spans in different processes are also suitable to carry out embedding and extraction in individual images. It may not be found suitable for implement video watermarking which involves a large number of frames run at a high speed. The ELM based approach is found very suitable both in terms of the optimization of the twin parameters as well as the time computation. The processing time is very less (milliseconds) and this makes it suitable to develop watermarking applications on a real time scale. Precisely due to this reason, in future, it may also be used in video watermarking.

IV. SUMMARY

Digital Watermarking can be used areas such as digital information where there is need for protection. This paper has given detailed review of various watermarking techniques. The use of Deep Learning with watermarking is the blooming area.

V. REFRENCES

[1] Chuan-Yu Chang and Sheng-JyunSu, A Neural-Network-Based Robust Watermarking Scheme, Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (2005) (Volume 3), 10-12 Oct, 2005, pp 2482-2487

[2] Cheng-Ri Piao, SeunghwaBeack, Dong-Min Woo, and Seung-Soo Han, A Blind Watermarking Algorithm Based on HVS and RBF Neural Network for Digital Image, ICNC 2006, Part I, LNCS 4221, (2006), pp. 493 – 496

[3] Cheddad, J. Condell, K. Curran and P. McKevitt, “Digital Image Steganography Survey and Analyses of Current Methods”, Signal Processing, vol.90, no.3, 2010.

[4] Vaishali S. Jabade and Dr. Sachin R. Gengaje, “Literature Review of Wavelet Based Digital Image Watermarking Techniques”, International Journal of Computer Applications, vol.31, no.1, 2011.

[5] Anurag Mishra, Amita Goel, Rampal Singh, Girija Chetty and Lavneet Singh, A Novel Image Watermarking Scheme Using Extreme Learning Machine, Proceedings of IEEE World Congress on Computational Intelligence (WCCI 2012), Brisbane, Australia, June 10-15, 2012, pp 1-6

[6] Song Huang, Wei Zhang, Wei Feng, Huaqian Yang, Blind watermarking scheme based on neural network, Seventh World Congress on Intelligent Control and Automation (WCICA 2008), 2008, pp. 5985–5989

[7] Shwu-Huey Yen and Chia-Jen Wang, SVM Based Watermarking Technique, Tamkang Journal of Science and Engineering (2006) ,Vol. 9, No. 2, pp 141-150

[8] Bibi Isac and V. Santhi, A study on Digital Image and Video Watermarking using Neural Networks, International Journal of Computer Applications, Vol. 12, No. 9, Jan 2011

[9] Aidin Ferdowsi_ and Walid Saad, Deep Learning-Based Dynamic Watermarking for Secure Signal Authentication in the Internet of Things, 3 Nov 2017.

[10] Xiaoyi Zhou ,1 Chunjie Cao ,1 Jixin Ma,2 and Longjuan Wang, Adaptive Digital Watermarking Scheme Based on Support Vector Machines and Optimized Genetic Algorithm, Hindawi Mathematical Problems in Engineering Volume 2018, Article ID 2685739.

[11] Nazir A Loani, Nasir N. Hurrah, Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption, Volume 6, 2018, Special Section on Information Security Solutions for Telemedicine Applications.

[12] Mayank Vatsa, Richa Singh and Afzal Noore, “Improving biometric recognition accuracy and robustness using DWT and SVM watermarking”, IEICE Electronics Express, vol.2, no.12, pp.362-367, 2005.

[13] Wu Jianzhen, “A RST Invariant Watermarking Scheme Utilizing Support Vector Machine and Image Moments for Synchronization”, IEEE International Conference on Information Assurance and Security, 2009.

[14] Lei Li, Wen-Yan Ding and Jin-Yan Li, “A Novel Robustness Image Watermarking Scheme Based on Fuzzy Support Vector Machine”, IEEE Pattern Recognition and Intelligence System, 2010.

[15] Yogendra Kumar Jain and Saurabh Tiwari, “An Enhanced Digital Watermarking for Color Image using SVM”, International Journal of Computer Science and Information Technology, vol.2, no.5, 2011.

[16] M. Vafaei, H. Mahdavi Nasab and H.Pourghassem,“A new blind Robust Watermarking method based on Neural Networks in Wavelet Transform Domain”, World Applied Science Journal, vol.22, no.11, 2013.

[17] Saadiah Yahya, Hanizan Shaker Hussain and Fakariah Hani M. Ali, “DCT Domain Stega SVM- shifted LSB Model for highly Imperceptible and robust cover image”, International Conference on Computing and Informatics, vol. 43, 2015.

[18] Lijing Zhang, Aihua Li, “A Novel Watermark Algorithm for Non-Compressed Digital Video”, 2nd International Workshop on Education Technology and Computer Science, 2010.