JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Survey on Digital Data Security Techniques and Attacks

Pawan Singh Rajput[1], Dr. Megha Kamble[2]

[1]Research Scholar, Department of Computer Science & Engineering, LNCT University, Bhopal, Madhya Pradesh, India.
[2]Associate Professor, Department of Computer Science & Engineering, LNCT University, Bhopal, Madhya Pradesh, India.

Abstract— Easiest medium for transferring of information from one place to other is digital. Many type of data like text, audio, video, image, etc. transfer by the same medium and by same techniques. Security of this data is highly depends on the protocols but some of precaution taken by the data owner by embedding some signature or validate information at receiver end. This paper has done a deep survey for methods proposed by researcher for digital image data security. Signature embedding techniques and its properties were detailed in the paper for improving the understanding of research area. In this paper various network attacks were also elaborate that may affects the received data. Various techniques like Least significant bit embedding, swapping, singular value decomposition, histogram sifting, etc. used by scholars for digital data securities techniques ~~were~~ are also explained in the paper, as each feature has its own importance and application area as per the type of image and attacks. This paper has finds that use of frequency domain features are more effective as compared to spatial feature set for embedding. Frequency feature increases the robustness of the signature against different spatial and geometrical attacks. It was also found that use of machine learning for detection of embedded portion is effective and fruitful in attack environment.

Keywords: Image Processing, Feature Extraction, Frequency Feature, Data hiding,

I. INTRODUCTION

Digital images are used to preserve important information. But providing integrity and authentication to these images is a challenging task as they are increasingly transmitted over insecure network such as internet. In this era with the use of fast advanced technologies it is easy to modify the contents of these digital images. Therefore there is need to protect these images against various attempts to manipulate them and it is important to make an effective method to solve image authentication problem that is ensuring the integrity of an image, particularly for document images such as important certificates, scanned cheques, art drawings, signed documents, circuit diagrams, design drafts etc.

With an increased concern in copyright protection comes an increased interest in digital watermarking. The internet, for the most part, is a user friendly place where people are interested in downloading pictures, music, and videos. The internet provides an efficient delivery system that is relatively inexpensive. Acquiring various media via the internet requires a fraction of the time it would take to go to a physical store to

purchase said media. Also, when one purchases media over the internet, one would only need virtual space to store the media in question as opposed to storing it on a shelf or wherever such media might be placed. Conversely, such ready availability provides people with the possibility of copyright violations. Digital Signature ("DS") is an electronic signature used to secure an electronic record or digital contracts. Like a traditional signature its purpose is to authenticate the document, thereby authenticating the parties to an agreement. It is used to ensure that there are no alterations in the original data while transferring them from sender to receiver. It has also become essential to authenticate the users often to ensure safety and to avoid fraud, DS cannot be imitated by anyone else hence provides protection. Basically, it provides legitimacy and assurance to the receiver that the message was generated by the known sender.

Paper second brief features used for embedding. Further third section has elaborate different work proposed by scholars in field of data security. Fourth section of paper detailed various essential characteristics of data hiding algorithms. In fifth section of paper different types of attacks were detailed that damage the signature in data. Finally paper concluded with different understanding and future scope.

II. Feature for Digital Image

Color feature: Image is a matrix of light intensity values, these intensity values represent different kind of color. so to identify an object colure is an important feature, one important property of this feature is low computation cost .

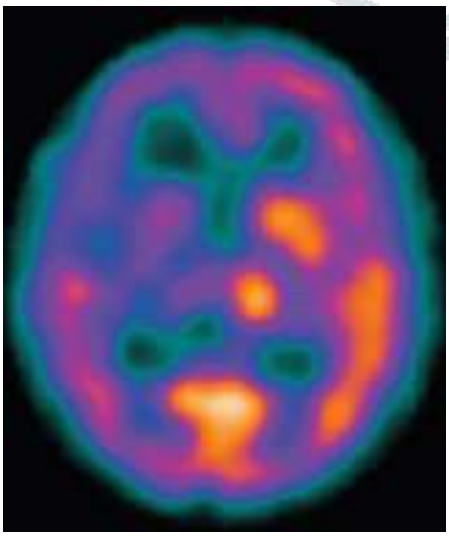

Fig. 1 Represent the HSV (Hue Saturation value) format of an image.

Different Image files available in different color formats like images have different colure format ranging from RGB which stand for red, green, and blue. This is a three dimensional representation of a single image in which two dimensional matrix represent single color and collection of those matrix tends to third dimension. In order to make intensity calculation for each pixel gray format is use, which is a two dimension values range from 0 to 255. In case of binary format which is a black and white color matrix whose values are only 0 or 1. With the help of this color feature face has been detected efficiently in [8].

Edge Feature: As image is a collection of intensity values, and with the sudden change in the values of an image one important feature arises as the Edge as shown in figure 4. This feature is use for different type of image object detection such as building on a scene, roads, etc [5]. There are many algorithm has been developed to effectively point out all the images of the image or frames which are Sobel, perwitt, canny, etc. out of these algorithms canny edge detection is one of the best algorithm to find all possible boundaries of an images.

Texture Feature: Texture is a degree of intensity difference of a surface which enumerates properties such as regularity and smoothness [1]. Compared to color space model, texture requires a processing step. The texture features on the basis of color are less sensitive to illumination changes as same as to edge features.

Histogram Feature: In this step image vector obtained after pre-processing is used where histogram of the image is find at one bins. This can be understand as let scale of color in fig. 4.2 is 1 to 10, than count of each pixel value is done in the image. So as per above vector Hi=[0, 0, 0, 4, 3, 5, 2, 1 2, 0] where H represent the color pixel value count and i represent the position in the H matrix with color value

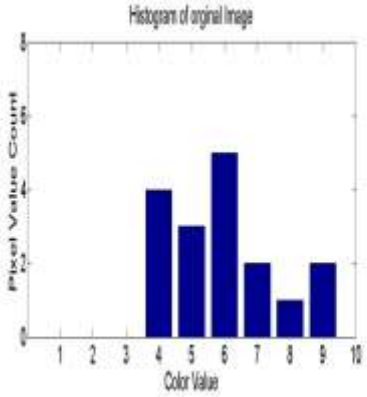

Fig. 2 Histogram of the original image.

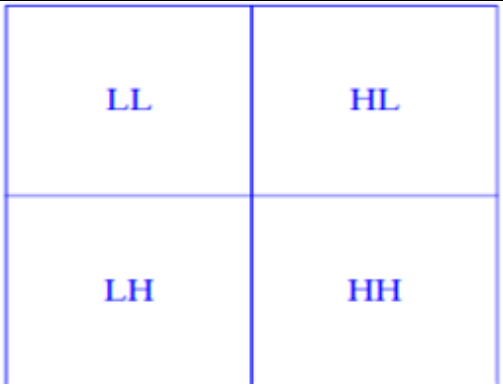

Fig. 3.4 DWT of image ~~from~~ [8].

Corner Feature: In order to stabilize the video frames in case of moving camera it require the difference between the two frames which are point out by the corner feature in the image or frame. So by finding the corner position of the two frames one can detect resize the window in original view. This feature is also use to find the angles as well as the distance between the object of the two different frames. As they represent point in the image so it is use to track the target object.

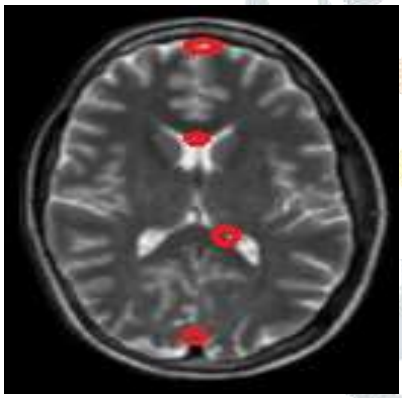

Fig 3 Represent the corner feature of an image with green point.

DWT (Discrete Wavelet Transform): LL: In fig. 4 upper left part is term as LL block. This block of image is obtain by filtering the image rows from the low pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain flat region of the image which do not have any edge information, so this is term as approximate version of the image.

HL: In fig. 4 upper right part is term as HL block. This block of image is obtain by filtering the image rows from the high pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain horizontal edge region of the image which do not have any flat information.

LH: In fig.4 lower left part is term as LH block. This block of image is obtain by filtering the image rows from the low pass filter then pass same to the high pass filter but here column are filter for the analysis. This block contain vertical edge region of the image which do not have any flat information.

HH: In fig. 4 lower right part is term as HH block. This block of image is obtain by filtering the image rows from the high pass filter then pass same to the high pass filter but here column are filter for the analysis. This block contain diagonal edge region of the image which do not have any flat information.

III. Related Work

Researcher are working in field of data security from last few decades, but as internet users increases chance of attack is high. This section of paper has summarized various scholars models of data embedding with techniques and features adopted.

In [4] paper, proposed a novel spatial domain color image watermarking technique is proposed to rapidly and effectively protect the copyright of the color image. First, the direct current (DC) coefficient of 2D-DFT obtained in the spatial domain is discussed, and the relationship between the change of each pixel in the spatial domain and the change of the DC coefficient in the Fourier transform is proved. Then, the DC coefficient is used to embed and extract watermark in the spatial domain by the

proposed quantization technique. The novelties of this paper include three points: 1) the DC coefficient of 2D-DFT is obtained in the spatial domain without of the true 2D-DFT; 2) the relationship between the change of each pixel in the image block and the change of the DC coefficient of 2D-DFT is found, and; 3) the proposed method has the short running time and strong robustness. Hashing information need to be replace as has hash value need to maintain for finding the embedded blocks.

In [5] has proposed a watermarking technique by embedding binary data in DCT full form whenever first time term is appearing middle band frequency region. In this paper image was blocked into fix size whereas per watermark bit DCT middle band fix co-ordinates values were swapped. Swapping of this was depend on certain conditions, so same set of conditions were maintained at receiver side for watermark extraction. This work face a low watermark absorption with low resistance against spatial attacks.

In [6] has proposed a between-class variance concept for embedding image in edge region of the image. Author has first apply discriminant analysis method for converting image into binary format, than apply BCV technique which classify pixel into edge and non-edge region. Change in spatial region of the image was done for hiding data into image edge region. In this model low space available for watermark while embedding in edge region is easy to trace the secret information.

In [7] author generates watermark from the input image only and embed in low frequency region of image were obtained by frequency features.. In this paper fragile watermarking technique was proposed which preserve images against JPEG compression attack. Paper has not cover other type of attack, while execution time of this work was also quite high.

In [8], author proposed a fractal code based self-reconstruction algorithm where input image was send in highly noisy area. So loss of information was assumed which was recovered by extra packets of fractal code. Tempering of image was also preserved to by hashing hash key as secret information. This paper has improve the robustness in lossy environment but it required extra bandwidth with computational complexity.

In [9] author has proposed a Singular value Decomposition technique to find resemble data in the original image. Authors of this paper divide image into fix size patch and replace those patch with KSVD patch. This increase the image security in network while encryption of watermark was also done before embedding. Here searching of correct patch from KSVD library was time taken. Dictionary storage at sender or receiver side was also bulky. In CNN was used for embedding the watermark data in original image. With the help of some supporting information it was found that Watermarking was extract from the image. Here it was obtained that both Watermarking and image got reverse at the receiving end.

In [10] author have proposed a novel blind watermarking technique using Back Propagation neural network in wavelet domain. In this paper, a scrambled watermark is embedded using the advantage of Human Vision System (HVS) to achieve better imperceptibility and robustness. Neural network is used to memorize the relation between the embedded watermark and corresponding watermarked image..

In [11] authors have proposed a novel image watermarking technique in multi-wavelet domain based on SVM. The algorithm have utilized special frequency band and the property of image for watermarking. Though the scheme is reasonably robust against various attacks but fails to achieve robustness against average filtering, median filtering, JPEG attacks and scaling attack effectively.

In [12] researchers have also proposed a robust technique in undecimated discrete wavelet transform (UDWT) domain using fuzzy SVM for geometric distortion correction. Though the technique provides adequate robustness, yet it requires excessive computational time and also it is not robust to local geometric distortions.

In [13] Third level LFT (Lifting Fourier transform) as used for embedding watermark. Feature set generated from the blocks in which reference watermark RW was embedded has been used as input feature vector in Feed Forward neural network. The corresponding bits of RW are used as target vector. The technique provides satisfactory robustness against different

attacks such as noising attacks, de-noising attacks, some geometric attacks, etc.

In [14] paper proposed the adaptive scaling factor based on selected DWT-DCT coefficients of its image content. The adaptive scaling factor was generated based on the role of selected DWT-DCT coefficients against the average value of DWT-DCT coefficients. The watermark image was embedded by using a proposed set of rules that consider the adaptive scaling factor.

In [15] propose a robust and reversible database watermarking technique, Genetic Algorithm and Histogram Shifting Watermarking (GAHSW), for numerical relational database. The genetic algorithm is used to select the best secret key for grouping database, where the watermarking can be embedded with balanced distortion and capacity. The histogram of the prediction error is shifted to embed the watermark with good robustness. Histogram shifting reduce the robustness of the work.

In [16] a digital watermarking system for neural networks was proposed. Authors formulate a new challenge: the integration of watermarks into neural networks through discrete cosine transform (DCT) based approach. For discrete wavelet transform (DWT)-based digital image watermarking algorithms, additional performance enhancements could be obtained by combining DWT with DCT. Throughout the neural networks, work also describe specifications, embedded conditions, and attack forms of watermarking.

In [17] authors presents a blind digital image watermarking technique in transform domain that uses probabilistic neural network (PNN) for the watermarking process. The proposed method aims to enhance the performance of watermarking using Probabilistic Neural-Network including three-level DWT and DCT transformations. In the embedding process, embedding of the watermark is done by training the PNN network. The new trained embedded values are used at the extraction side and inverse three-level DWT and DCT are applied. The inverse transformation will give the extracted watermark.

In [18] GAN (generative adversarial networks) based approaches have gained traction, popularised by the HiDDeN model, which was the first end-to-end trainable model for digital watermarking and steganography. These deep learning models employ different message embedding strategies in order to improve robustness, such as using adversarial examples, attention masks, and channel coding. The continued development of deep learning-based data hiding models will greatly improve the effectiveness and security of digital IP protection, and secure secret communication

Robust and blind digital watermarking results can be achieved using a relatively shallow network, as was shown by WMNet [19]. The watermarking process is separated into three stages: watermark embedding, attack simulation, where the CNN adaptively captures the robust features of various attacks, and updating, where the model's weights are updated in order to minimise the loss function and thereby correctly extract the watermark message. Embedding is achieved by increasingly changing an image block to represent a watermark bit. The model is trained to extract watermark bits from the image blocks after attack simulations have been applied.

ReDMark [20] uses two Full Convolutional Neural Networks (FCNs) for embedding and extraction along with a differentiable attack layer to simulate different distortions, creating an end-to-end training scheme. ReDMark is capable of learning many embedding patterns in different transform domains and can be trained for specific attacks, or against a range of attacks. The model also includes a diffusion mechanism based on circular convolutional layers, allowing watermark data to be diffused across a wide area of an image rather than being confined to one image block. This improves robustness against heavy attacks, because if one image block is cropped out or corrupted, the watermark can still be recovered. The trade-off between robustness and imperceptibility can be controlled via a strength factor that can influence the pattern strength of the embedding network.

Above discussion of different models proposed by scholars has found that most of work use frequency domain features for embedding, while spatial feature are less effective. Scholars are using neural network in the hiding technique for increase the detection accuracy of digital signature.

IV. Data Security Algorithm Properties

The following are some significant parameters to consider while creating universal digital image security :

Fidelity: This refers to the fact that the image's watermarking should not be apparent to humans, and that images should not alter before or after the watermarking procedure.

Robustness refers to an image's capacity to withstand multiple processing attacks without being harmed. These assaults are frequently carried out in order to disrupt the watermark in order to complete the intended activity. Cryptographic attacks, removal attacks, geometric attacks, and protocol assaults are all examples of such attacks [21]. Watermarking algorithms can't withstand all kinds of attacks. Although robust watermarking is not required in all applications, it is required in certain of them.

Data Payload (or Capacity) is a notion that allows a number of bits to be buried in any image without compromising the image's quality. It's also a consideration of how many bits can be stored in a picture and simply removed when needed. The capacity for embedding may vary depending on the application.

Security refers to an image's ability to withstand external threats. The watermarking system must be safe enough that any unauthorized individual who does not know the algorithm will be unable to extract the information. Only a trusted individual should be able to remove the watermark. [20]

Computational Complexity: This refers to the amount of time it takes to extract and embed the watermark. Some real-time applications are quick, but when a high level of security is required, it takes some time to use complicated algorithms.

Perceptibility: This parameter indicates how much of an image is degraded when the watermark is embedded. In an invisible watermarking technique, it's best to maintain this parameter as low as feasible. [13]

Imperceptibility: This phrase refers to the invisibility necessary in such watermarking systems. This feature specifies that the original and watermarked images should be similar[20], which can be accomplished by lowering capacity, robustness, or both. The basic benchmark for measuring the imperceptibility of any image is the Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM) index [13]

V. Attack on Image

Compared to wired networks, the WSNs that deploy in the extreme environment face more threats, and what is more, the public communication protocol adopted by WSNs exacerbates the risk of physical tampering [22, 23]. The sensed node owns limited computational capabilities and energy resources which increase the difficulty of designing security protocols. We summarize the main attack models into five categories:

(a)Packet tampering: a malicious node added to WSNs tampers with the value of the packets and forwards the tampered packets which can lead to extremely serious consequences in some special cases.

(b)Packet forgery: a malicious node added to WSNs keeps sending the fake packets to other nodes, greatly increasing network traffic and resulting in wasting energy of the whole WSNs.(c)Selective forwarding: a malicious node added to WSNs deletes partial packets and forwards some packets to destination selectively. The data loss may cause the bad situation that the sink node fails to make the correct response.

(d)Packet replay: a malicious node added to WSNs forwards the packets that have been forwarded, once more or repeatedly to other nodes which will cause the traffic congestion and energy waste.

(e)Transfer delay: a malicious node added to WSNs forwards the packets later than the predetermined time which will lead to the fact that the sink node drops the packets due to the timestamp.

Conclusions

Data has many states storage, transfer, transformation, etc. at each state authenticity of data is highly required. Tampering in hard data is easy to detect but in case of digital its get tough to identify and authenticate. This paper has work in field of digital data security by summarizing various work proposed by scholars with adopted techniques. To increase the topic understanding

features were list with their uses. As attacks in these age is common, hence different attacks were also detailed in the paper those should be keep in mind while developing data security algorithm. It was found that many of scholars are using neural network in data security apart from traditional algorithms like embedding in least significant position of data. Further researchers are using visual features for embedding as they support invisible hiding. Scholars should use frequency domain feature like DWT, DCT for hiding to increase robustness. In future scholars can proposed a model that makes less impact on input data for retaining the originality.

References

1. X. Sun, J. Su, B. Wang, and Q. Liu, "Digital watermarking method for data integrity protection in wireless sensor networks," International Journal of Security and Its Applications, vol. 7, no. 4, pp. 407–416, 2013.
2. David Ifeoluwa Adelani, Haotian Mai, Fuming Fang, Huy H. Nguyen, Junichi Yamagishi, and Isao Echizen. 2019. Generating Sentiment-Preserving Fake Online Reviews Using Neural Language Models and Their Human- and Machine-based Detection. (2019).
3. Beijing Chen, Jiaxin Wang, Yingyue Chen, Zilong Jin, Hiuk Jae Shim, and Yun-Qing Shi. 2020. High-Capacity Robust Image Steganography via Adversarial Network. KSII Transactions on Internet & Information Systems 14, 1 (2020).
4. 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.
5. Mohammed A. M. Abdullah, Satnam S. Dlay, Wai L. Woo, and Jonathon A. Chambers. "A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography". IEEE Access Year: 2016, Volume: 4 Pages: 10180 – 10193.
6. Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ And Shigeo Kato . "Digital Image Watermarking Method Using Between-Class Variance". 978-1-4673-2533-2/12/$26.00 ©2012 IEEE.
7. Angela Piper1, ReihanehSafavi-Naini. "Scalable Fragile Watermarking For Image Authentication". Published In IET Information Security, On 31st December 2012.
8. Paweł Korus, Student Member, IEEE, AndAndrzejDziech. "Efficient Method For Content Reconstruction with Self-Embedding". IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 3, MARCH 2013.
9. HaniehKhalilian, 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.
10. S. Huang, W. Zhang, W. Feng and H. Yang, Blind watermarking scheme based on neural network, Proceedings of the 7th IEEE World Congress on Intelligent Control and Automation (2008), 5985–5989.
11. H. Peng, J. Wang and W. Wang, Image watermarking method in multiwavelet domain based on support vector machines, Journal of Systems and Software 83(8) (2010), 1470–1477.
12. H.Y. Yang, X.Y. Wang and C.P. Wang, A robust digital watermarking algorithm in undecimated discrete wavelet transform domain, Computers and Electrical Engineering 39(3) (2013), 893–906.
13. MohiulIslama,∗, AmarjitRoyb and RabulHussainLaskar. "Neural network based robust image watermarking technique in LWT domain". Journal of Intelligent & Fuzzy Systems 34 (2018) 1691–1700.
14. Ferda Ernawan, Dhani Ariatmanto, And Ahmad Firdaus. "An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients", March 29, 2021.
15. Donghui Hu, Dan Zhao, ShuliZheng. "A New Robust Approach for Reversible Database Watermarking With Distortion Control". IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, 2019.
16. R. S. Kavitha, U. Eranna, M. N. Giriprasad. "An Image Compression Based Technique to Watermark a Neural Network". (IJITEE) ISSN: 2278-3075, Volume-9 Issue-4, February 2020
17. Suresh Kuri, Gururaj Kulkarni. "Robust Digital Image Watermarking using DWT, DCT and Probabilistic Neural Network". International Conference on

Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), 2017.

18. Linfeng Geng, Weiming Zhang, Haozhe Chen, Han Fang, and Nenghai Yu. 2020. Real-time attacks on robust watermarking tools in the wild by CNN. Journal of Real-Time Image Processing 17 (6 2020).

19.] Seung-Min Mun, Seung-Hun Nam, Haneol Jang, Dongkyu Kim, and Heung-Kyu Lee. 2019. Finding robust domain from attacks: A learning framework for blind watermarking. Neurocomputing 337 (2019), 191–202.

20. Mahdi Ahmadi, Alireza Norouzi, S. M. Reza Soroushmehr, Nader Karimi, Kayvan Najarian, Shadrokh Samavi, and Ali Emami. 2020. ReDMark: Framework for Residual Diffusion Watermarking on Deep Networks. Expert Systems with Applications 146 (2020).

21. Srivastava Kumar Sumit, Pandey Harikesh."Medical Image Watermarking with Patient Details as Watermark". International Journal of Advance research, Ideas and Innovations in Technology, Volume2, Issue6, 2016.

22. A. Gutub and M. Al-Ghamdi, “Hiding shares by multimedia image steganography for optimized counting-based secret sharing,” Multimedia Tools and Applications, vol. 79, no. 11-12, pp. 7951–7985, 2020.

23. K.-H. Jung, “Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane,” Journal of Real-Time Image Processing, vol. 14, no. 1, pp. 127–136, 2018.

24. Jain M, Lenka SK (2016) Diagonal queue medical image steganography with rabin cryptosystem. Springer Brain Inform 3(1):39–51.