Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 02, February-2018

Framework for Improvising Dual Digital Watermarking through Deep Learning Techniques

G. Saranya
P.G. Scholar,
Department of Computer Science and Engineering
Rajalakshmi Engineering College, Chennai

Mrs.Priya Vijay
Associate Professor,
Department of Computer Science and Engineering,
Rajalakshmi Engineering College, Chennai.

***Abstract*--- Image watermarking has come through lot of improvisation over two decades still it provides number of research dimension is related to the compression rates, robustness against attacks and high security for privacy data. Achieving better compression rates in dual digital watermarking is still area of concern. Digital watermarking has four techniques for compression the image. The paper explains the state of art for all four techniques and reveals the importance of embedding of fragile and robust watermark during compression on the image encoder. The respective embedding approach on the image is termed as optimized compression/ watermarking algorithm and system. The papers also propose a framework with Deep learning techniques to improvise the existing systems.**

Keywords---Watermarking, Fragile and robust watermarking, Deep learning techniques,

I INTRODUCTION

Watermarking is the process of data hiding that is combination of steganography and cryptography which means communication of information by embedding it in and retrieving it form other digital data. Image watermarking has come through lot of improvisation over two decades still it provides number of research dimension which relates to the compression rates, robustness against attacks and high security for privacy data. Digital watermarking(DWM) is a passive protection tool, watermark is embedded into a cover image in such a way that the resulting watermarked signal is robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment

A watermarking system is divided into three steps embedding, attack, and detection. In embedding Process, an algorithm accepts data to be embedded, Host and produces a watermarked signal. The watermarked digital signal is transmitted to another person. If this person makes a modification, then it is termed as attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. Watermarking undergoes many possible modifications such as lossy compression of the data, image or video is cropped, or intentionally adding noise to the data. Detection also called as extraction is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. During transmission if the signals are unmodified, then the watermark still is present and it may be extracted

Security methods in watermarking is crack by the cryptographic attacks and hence its finds a way to remove the information that is embedded in WM or to embed false watermarks. Brute-force is one of the technique that is used to embed the secret information. This type of attacks is restricted due to their high computational complexity. They cover, for example, direct attacks to find the secret key or attacks called collusion attacks. Cryptographic attacks are very similar to the attacks used in cryptography. There are the brute force attacks, which aim at finding secret information through an exhaustive search. Since many watermarking schemes use a secret key, it is very important to use keys with a secure length. Oracle attack is another type in this category which is used to create a non-watermarked image when a detector device is available in watermark.

II STATE OF ART

Xiao-Long Liu, Chia-Chen Lin, Shyan-Ming Yuan [1] conducted study on blind dual watermarking for copyright protection invisible robust watermarks are embedded and for image authentication fragile watermarks are embedded. Watermark image is first embedded by using the discrete wavelet transform (DWT) in YCbCr color space, and the host image is blindly extracted. However, fragile watermarking is upgraded based on least significant bits (LSB) which is the replacement approach in RGB components for authentication of image. Without the host image authenticity and integrity of a suspicious image can be verified blindly and the original watermark. The proposed structure suitable 1for cover the valuable original images by the combination of robust and fragile watermarking.

In 2014 Myasar Mundher1, Dzulkifli Muhamad1 and Amjad Rehman [2] conducted researches saying that Digital watermark is the process of holding the data in the document that contains the host images, to authenticate the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 02, February-2018

identity of its owners and authentication of the data. The digital data might be images, audios or videos that is embedded information could be an image or textual data, to authenticate the data ownership such as the name of the author, signature, enterprise logo etc. From watermarked images the watermark is extracted and detected to authenticate the original owner.In the host image the watermark is embedded that is used by owners to claim that the multimedia data that is belongs to watermark that cannot be easily removed from images which protect the intellectual belongings of images, audio and videos, watermark W is converted into a sequence of bits and encryption is done on the watermark image, sequence of size R is selected randomly. In addition a random pseudo number is generated to determine the corresponding pixels for selection key generation. Finally, 2-level discrete slanlet transform (DST) on the host image is applied to divide it into Red, Green and Blue channels.

The study by Ramandeep Kaur[3] on digital information such as image, video, audio or text are to be stored, transmitted and distributed through internet without any loss or damage of data. This type of work performs the hybrid DWT-SVD technique with the concept of entropy. The concept behind the proposed technique is based on fusing multiple watermark images using wavelet fusion algorithm. Original image is initially splits into blocks. Then the high entropy blocks are selected for embedding fused watermark in original image. That fused watermark is to be embedded in high entropy areas of the image using Hybrid DWT-SVD Technique. The work of proposed technique is evaluated and comparative analysis is done by Hybrid DWT-SVD and Hybrid DWT-SVD with concept of entropy, Digital Image processing is a approach which contains image data to be scanned and calculated. The image processing have digital image processing, indexing of images, scanning the digital edition of image processing, service evaluation of the image using the latest technology. Digital media technology has a wide range of Internet as well as wireless applications. However, the distribution and use of multimedia data is faster and easier with success of the Internet. A digital image is a image of a 2-D representation, as the resolution of the image is fixed. It can be vector type or can be the frame type. A digital watermark is a type of brand that can be integrated into the signal is noise tolerant as audio, video, image, etc. Basically, the mechanism of watermarking is to hide information in digital carrier signal, but it does not relates with the carrier signals. Imperceptible, robustness and capacity are the three basic types of specification in watermarking. The watermarking process includes steps which are embedding, attack and extraction process. Embedding is an algorithm which accepts the host and does integration of data, and produces a signal which is watermarked.

In 2017 Seung-Min Mun, Seung-Hun Nam [4]conducted the study stating that Convolutional neural network (CNN) is the process of iterative learning framework in order to protected robustness of watermarking image. In CNN the loop of learning process consists of the following three stages: Watermark embedding, attack simulation, and weight update. Need to analyze the network that can detect a 1-bit message from a sub-block of images. CNN has adequately large number of layers and filters can be seen as a generalization of QDFT and QIM. In order to construct a CNN model that proceeds with R×C size block as input and determines a message bit. This CNN is then used in a similar way to QDFT in traditional frequency domain watermarking techniques. Training comprises three stages starting from a CNN with random weight. A CNN model modified from a part of the most powerful model called Residual Network, which includes residual units and batch normalization.

The study by Mr. Bhupendra Ram Mr. Manoj Kumar[5] proven that Digital watermarking(DWM) has advanced result to copyright protection and authentication of multimedia data in a networked environment, since it provides the viable to identify the author, owner, distributor or authorized consumer of a document. In this paper a new watermarking technique to add a code to digital images, this method operates in the frequency domain embedding a pseudo-random sequence of real numbers in a selected set of DCT coefficient. And a new method does not require the host image for detection of watermarking. In The image coefficients are added to the watermark is added with significant image energy in the transform domain, this process is done to ensure usability of the watermark. Utility of the proposed method includes the enhanced resistance to attacks on the watermark, the Digital watermarking is validates by the frequency wavelet transform and the threshold frequency of the image, which provides the solution for a developers to provide value added protection on top of data encryption and scrambling for content protection. Hidden copyright information or other verification message are individually added to the watermarking image. Watermarking is the mechanism that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. Digital watermark is classification information containing the copyright for the multimedia data.

In 2015 Zhu Yuefeng, Lin Li [6] stated that dual watermarking is the process of inserting two value image watermarking. In this proposed work, the watermark information and gray image watermarking are inserted.In the carrier image on the dual watermark includes a two watermark image and a gray image watermarking algorithm, the main objective is maintaining the original two values of the watermark and robustness at the same time,hence it improve the watermark information. Embedding position is change to balance the robustness and invisibility of watermarking algorithm and also improve the strategy of transform domain algorithms, in the carrier image the DC coefficient is divided into blocks of DCT spectrum and spectrum with DWT combination.The advantage of embedded dual watermarking is that improve the adaptiveness based on the embedded mode. The gray image watermark bit plane decomposition compression high

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 02, February-2018

four bit plane information as watermarking, in reducing the original watermark loading and enhance the overall strength of self recovery system. Digital watermarking has classification of digital watermarking, attack types, performance index, and evaluation method. DCT transform and Arnold transform are the simulation study of digital watermarking algorithm , the algorithm's imperceptibility, robustness and security are analyzed, the algorithm for embedding process.

K.Haribabu, Deepak Mishra [7] conducted the study on Watermarking which plays a significant role in maintaining authentication, ownership and secret information that is trasmitted. Spatial domain or transformation domain are existing system in watermarking. Convolutional Neural Networks (CNN) were expand in early 90s and became popular and it has been use for wide range of application like classification, detection, recognition, patch matching. In propose work a digital image watermarking technique using auto-encoder based CNN which is robust to different noises and attacks like salt & pepper, CNN has adequately large number of layers and filters can be seen as a generalization of QDFT and QIM. In order to construct a CNN model that proceeds with R×C size block as input and determines a message bit. This CNN is then used in a similar way to QDFT in traditional frequency domain watermarking techniques. Training comprises three stages starting from a CNN with random weight. A CNN model modified from a part of the most powerful model called Residual Network, which includes residual units and batch normalization.

Mehran Andalibi and Damon M. Chandle [8] conducted the search on One of developed area of digital image watermarking is Grayscale logo watermarking, which is embed as a smaller logo in the host image. The main benefits of this is approach ability to visually and analyze the extracted logo for rapid visual authentication and other visual tasks. However, invisible watermarking applications logos pose new challenges, which need to keep the watermark is invisible within the host image which is used simultaneously maintaining robustness against the attacks. The proposed algorithm for invisible grayscale logo watermarking can operates via adaptive texturization of the logo. The important idea of this approach is to modify the watermarking task into a texture similarity task. The first step is to separate the host image into sufficiently textured and poorly textured regions.later, for textured regions,logo is transform into a visually similar texture via the Arnold transform and one lossless rotation; whereas in poorly textured regions,only a lossless rotation are used. The iteration for the Arnold transform and the angle of lossless rotation are determined by a model of visual texture similarity. Using standard wavelet, logo are transformed into that region via an embedding scheme.Multistep extraction stage are used for parameter estimation to perform geometrical transformations. Testing with multiple logos on a database of host images and under a variety of attacks demonstrates that the proposed algorithm yields better overall performance than competing methods.

III FRAMEWORK MODEL

The proposed system implements Convolutional Neural Network(CNN) is the deep class that is it is implemented by Forward Neural Networks(FNN) which is used to analysis the visual image .CNN consists hidden layer it has input and output layer.

CNN is fully connected that is used to learn or to classify the data. CNN architecture consists of high numbers of neurons, each neurons in the layers are connected to neurons of another layers. Convolutional Neural Network contains one or more Convolutional layers it also has one or more fully connected layers.

CNN architecture has the advantage of 2D structure of the input image that is accomplished with local connections and tied weights. Another advantage of CNN is easy to train the parameters in the connected networks and the numbers of hidden units in the networks Convolutional Neural Network is implemented in three stage are Embedding the watermark, Attack simulation and Weight update Watermarking is applicable of embedder and detector that is implemented by CNN, embedding is the process of learning and CNN detector extracts the message bit from the hidden blocks.

Implementation of three layer is important in system design are input image, hidden layer and output image, input image is splited into abstraction of hidden layer. The hidden layer are rearrange with the pixels and transmitted to the CNN encryption, two different type of keys are used for encryption and decryption of the image. Pooling layer is used for transmission of image with the rearrages pixels.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 02, February-2018

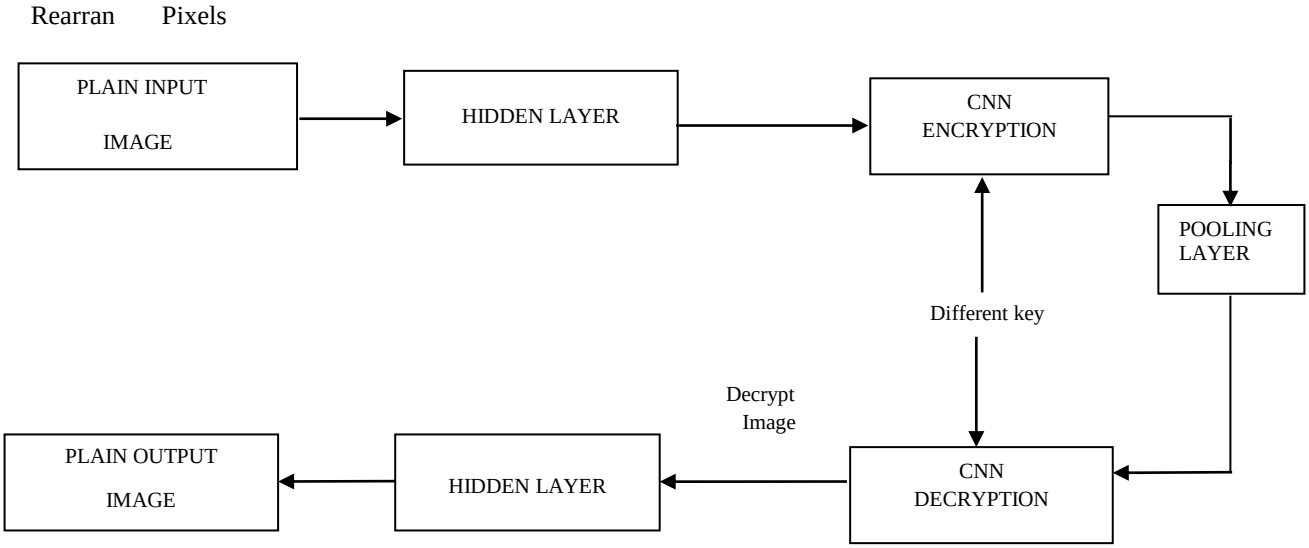

Fig1 Architecture diagram

IV CONCULSION:

Digital Image watermarking has come through lot of improvisation over two decades still it provides number of research dimension which relates to the compression rates, robustness against attacks and high security for privacy data. "Achieving better compression rates in dual digital watermarking" is still area of concern. Digital watermarking(DWM) is a passive protection tool, that is watermark is embedded into a cover image in such a way that the resulting watermarked signal is robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment. The main objective of the method is to automatically segment and detect Authentication and copy right protection of the image using convolution Neural Network (CNN). Accurate detection of size and location of segmentation plays a vital role .The proposed work is more successful in order to overcome, the conventional algorithm drawbacks and more suitable to applied in the real time applications.

REFERENCE

[1] Xiao-Long Liu, Chia-Chen Lin, Shyan-Ming Yuan:"Blind dual watermarking for color image authentication and copyright protection", IEEE Transactions on Circuits and Systems for Video Technolog,Vol 99, December 2016.

[2] Myasar Mundher1 , Dzulkifli Muhamad1 , Amjad Rehman, "Digital watermarking for image security using discrete slantlet transform", Applied Mathematics & Information Sciences, Nov2014.

[3] Ramandeep Kaur, Amandeep Kau,"Hiding copyright mark in image using watermarking technique",International Journal of Advanced Research in Computer Science and Software Engineering,Vol 4, May 2015.

[4] Seung-Min Mun, Seung-Hun Nam, "A robust blind watermarking using convolutional netural networks", International Journal of Computer Application, April 2017.

[5] Mr. BhupendraRam, Mr. Manoj Kumar, "Digital image watermarking technique using dwt and dct", International Journal of Advancements in Research & Technology, Vol 2, April-2016.

[6] Zhu Yuefeng, Lin Li, "Digital image watermarking algorithms based on dual transform domain and self recovery", International Journal on smart sensing and intelligent system, Vol. 8, March 2015.

[7] K.Haribabu, Deepak Mishra, "A robust Digital image watermarking technique using auto encoder base cnn", IEEE workshop on computer intelligence theories, June 2016.

[8] MehranAndalibi and Damon M.Chandle, "A Digital image watermarking via adaptive logo texturization", IEEE Transactions on Image Processing, vol 24, December 2015.