ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 12, December 2020

Rugged Picture Watermarking Using Knowledge Engineering

[1] Anu Jangraa, [2] Rekha
[1] Department of computer science and Engineering , Sushant University, Gurgaon

Abstract: In the digital information age, digital documents such as text, photo , audio, video and 3D computer graphics models can be easily copied, manipulated and distributed over the open channel. Recently, many new techniques have been widely used to protect the multimedia data transmission, storage, sharing and processing of digital contents. The aim behind attacks can be to alter, change, or delete the digital contents to illegally claim ownership or preventing the information transfer to intended recipients. The digital watermarking techniques offer a valuable solution to these problems. The watermarking is a data hiding technique for inserting digital data, also known as watermark, into digital documents, which can be later extracted or detected for the purposes of identification and authentication in many applications. Robustness, imperceptibility, capacity, safety and computational cost are the major benchmark parameters for general watermarking system. However, there exists some trade-off between these parameters of the watermark. Therefore, some optimization methods are required to balance these benchmark parameters. In past years, different artificial intelligent techniques are used as an optimization technique to offer the optimal balance between visual quality of the watermarked image and the robustness of the extracted watermark.

Keywords:- Reversible Color-to-grayscale Conversion, watermarked image, robustness

I. INTRODUCTION

From last few years growth in technology of computers and computer networks provides quality of service and higher bandwidth for both wireless and wired networks. However the representation of media in digital form and evolution of internet also made easy to transmit digital media such as pictures, audio, video in an effortless way. These advancements also raised some security related issues for the protection of multimedia data and require some data hiding techniques. The aim of data hiding is not to restrict the access to host signal, but to ensure that the embedded data should be inviolate and recoverable. There are two methods for data hiding: Steganography and Watermarking. Steganography is defined as the technique of hiding communication, the hidden content is embedded in some image so that there will not be any eavesdropper suspicion. Watermarking is one of the new techniques that provide protection against various attacks, data authentication and security to digital media. It is the process of embedding secret data in the form of signal called watermark into digital media (i.e. pictures, audio and video) so that this secret information can detected and extracted out to check the real owner or identity of digital media. Watermarking is very same to steganography with additional requirement of robustness. In watermarking system watermark is embedded in such a way that it cannot be changed without making whole cover image meaningless. Applications of Digital Watermarking Digital watermarks are playing very good role in various applications

Described below:

(1) Copyright Protection: Watermarking is used for the protection of copyrighted material over not secure network. Networks like internet or peer-to-peer (p2p) networks have watermarking methods to detect the copyrighted material from these networks.

(2) Content Archiving: Watermarking can be used to add an identifier or serial number for archiving digital objects such as pictures, audio and video. Usually filenames are used as identifier for classifying digital objects which are fragile and can be easily changed. Therefore watermarks can be mostly used as identifier for classification and reduces tampering.

(3) Meta-data Insertion: Watermarks can be used to add metadata which is used to describe data. Images are used in search engines are labeled with their content. Pictures are used by journalists to insert story of their news. In medical application x-rays store patient record.

(4) Broadcast Monitoring: It refers to the methods of checking whether the content that is broadcasted is same as the content that was expected to be broadcasted. Watermarking has major application in monitoring advertisement broadcasting.

(5) Tamper Detection: Fragile watermarks are used to find out tampering and unauthorized access. It has very important application in saving sensitive data like satellite and medical images. Tamper detection is used in court to

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 12, December 2020

prove whether the image is tampered or not Characteristics of Watermarking.

The important characteristics of watermark are described here:

1. Robustness: It is the ability in which watermark should survive from many signal processing, geometrical and malicious attacks.
2. Imperceptibility: The watermark should not be observed and seen by human and only be detected by watermark extraction process.
3. Verifiability: Watermark should give full evidence of the owner of copyright protected digital data. It can be used for authentication and control illegal copying.
4. Security: The watermark should be very secure so that any hacker cannot remove watermark without knowing the embedding algorithm and strength of watermark. This is generally achieved by security keys which can be either asymmetric keys or symmetric key.
5. Computational cost: Watermarking method should not be very complex so that its computational cost remains less. If the watermarking algorithms are very complex they require more computational cost.
6. Capacity and data payload: Capacity can be defined as maximum amount of information in the form of watermark that can be embedded in main image. Number of watermark bits in the message is called data payload and number of times the data payload is repeated is called watermark capacity. These characteristics are important because based on them various watermarking methods are classified. The performance of these watermarking methods is evaluated based on important factors which are robustness and imperceptibility.

Various spatial domain techniques are:

1. Least significant bit (LSB): It is commonly used spatial domain technique in which randomly pixels of cover image are selected and watermark is embedded in least significant bits. For e.g. Image: 10001000 10101001 11100011 11001100 Watermark: 1 0 0 1 Watermarked image: 10001001 10101000 11100010 11001101 5
2. Predictive Coding Schemes: This technique is more robust as compared to LSB. In this technique correlation between adjacent pixels is found. First set of pixels need to be embedded with watermark is taken and then difference between adjacent pixels is used to replace alternate pixels. At the receiver end cipher key is used for the retrieval of watermark.
3. Correlation-Based Techniques: In this technique a pseudo-random noise is added to an image and during decoding a correlation between two is found. If correlation value exceeds some threshold level watermark is found otherwise it is not.
4. Patchwork Techniques: This technique partitions image into two subsets. Some operation is then applied to these subsets in opposite direction. For example if one subset is decreased by factor x, the other subset should be increased by same amount.

Various transform domain techniques are :

1. Discrete Cosine Transform (DCT): DCT of digital image provides frequency space . DCT coefficients for an input image (I) of size N×N are computed according to Eq. (1). D (i, j) is the DCT coefficient in row i and column j of the DCT matrix and I (x, y) is the intensity of the pixel in row x and column y of the image.

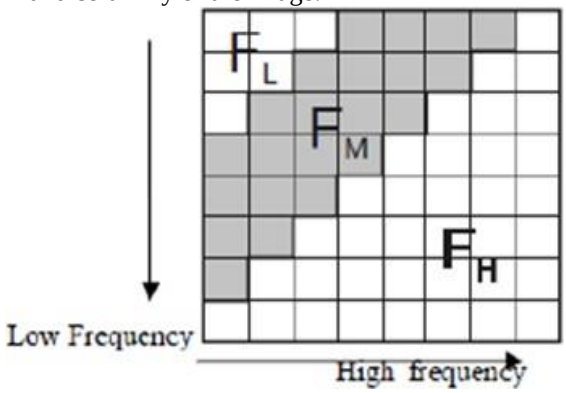


Figure 1.1: Discrete Cosine Transform Region

1. DWT of digital image provides multi- resolution representation of an image which helps in interpreting image information . It transforms the two-dimensional digital image into four quadrants of different frequencies i.e. LL1, LH1, HL1, HH1.
2. DFT provides robustness against various geometrical attacks like rotation, scaling, translation etc. DFT decomposes image into sine and cosine form. DFT magnitude and phase coefficients are modified while embedding watermark.

Artificial Intelligence techniques:

1. Back propagation neural network:

A typical neural network consists of an input layer, hidden layers and output layer. Number of nodes in input layer is determined by number of input and output

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 12, December 2020

variables. Each node is fully connected to its adjacent layers through links. Each link has weighting value to represent relational degree between two nodes.

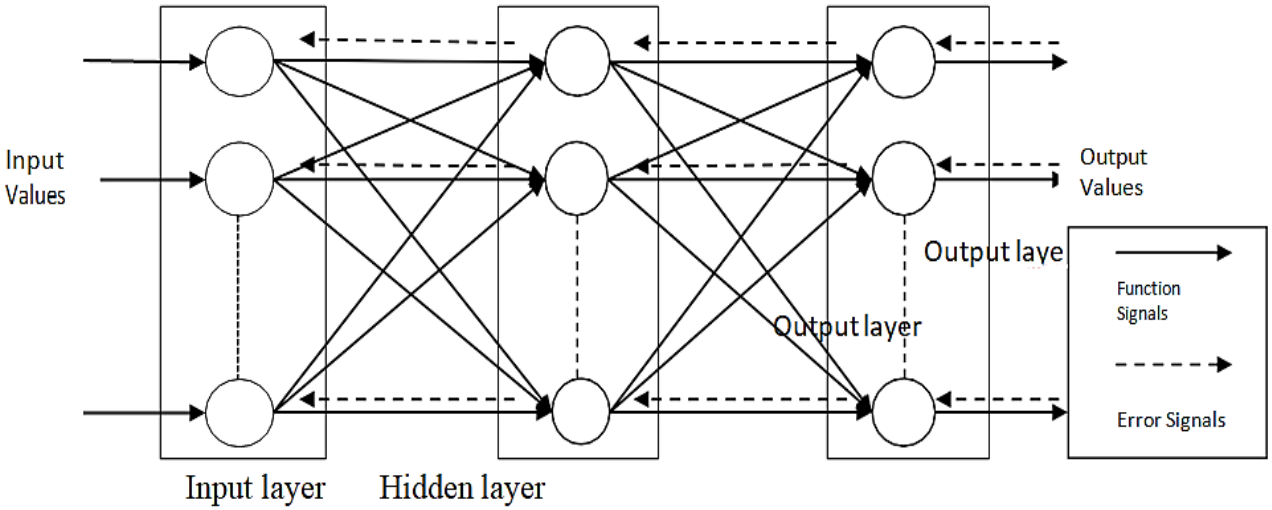


Figure 1.2: Back Propagation Neural Network

II. GENETIC ALGORITHM

Genetic Algorithm (GA) is widely used as an optimization method. It is a searching algorithm based on natural selection and genetics. GA uses population, which is composed of group of chromosomes to represent solution of system. Then fitness function is used to evaluate the fitness of each chromosome.

III. DIFFERENTIAL EVOLUTION

Differential Evolution (DE) is optimization algorithm that can be used to minimize non- differentiable and non-linear continuous functions with real-valued parameters. It resembles the structure of evolutionary algorithm, but differs in generation of new candidate solutions and by its use of greedy selection scheme.

IV. PARTICLE SWARM OPTIMIZER

It is an evolutionary algorithms, a population of particles is randomly generated then by using iterative search optimum is found.Each particle

Output laye

Output layer

Is associated with velocity vector and position vector.

Embedding algorithm :

1.Apply third level DWT transform on cover image to decompose it into corresponding sub bands.

2.Select LL3 sub band and Apply SVD on red ,

Green and blue components on cover image.

$A_{ci} = U_{ci}S_{ci}V_{ci}^{T}$ i = R, G & B

3.Apply SVD on red , green and blue components on watermark image to obtain its corresponding matrics.

$A_{wi} = U_{wi}S_{wi}V_{wi}^{T}$ i = R, G & B

4. Modify the singular values of different color components LL3 sub band of cover image with the singular values of different components of watermark image.

$S_{wati}=S_{ci}+k*S_{wi}$

.5. Obtain modified LL3* sub band using following equations.

Awati = Uci * Swati * Vci T

6. These arrays (A_{watr}, A_{watg}, A_{watb}) are concatenated in three dimension to obtain modified $LL3^{*}$ sub-band.

7.Change LL3 subband with modified LL3 * at third level and apply inverse IDWT to get watermarked image.

8. Apply attacks and noise to the watermarked image to check the robustness of the proposed algorithm.

Extraction algorithm :

1. Apply third level DWT transform on cover image to decompose in to sub bands.

2.Select LL3 subband and apply and apply SVD on red , green and blue components on cover image .

$A_{ci} = U_{ci}S_{ci}V_{ci}^{T}$ i = R, G & B

3.Apply SVD on red, green and blue components of watermark image.

Awi=UwiSwiVwiT

4. Apply step 1 and step 2 on watermark image to obtain its corresponding SVD matrics on LL3 subaband.

Awati=UwatiSwatiVwatiT

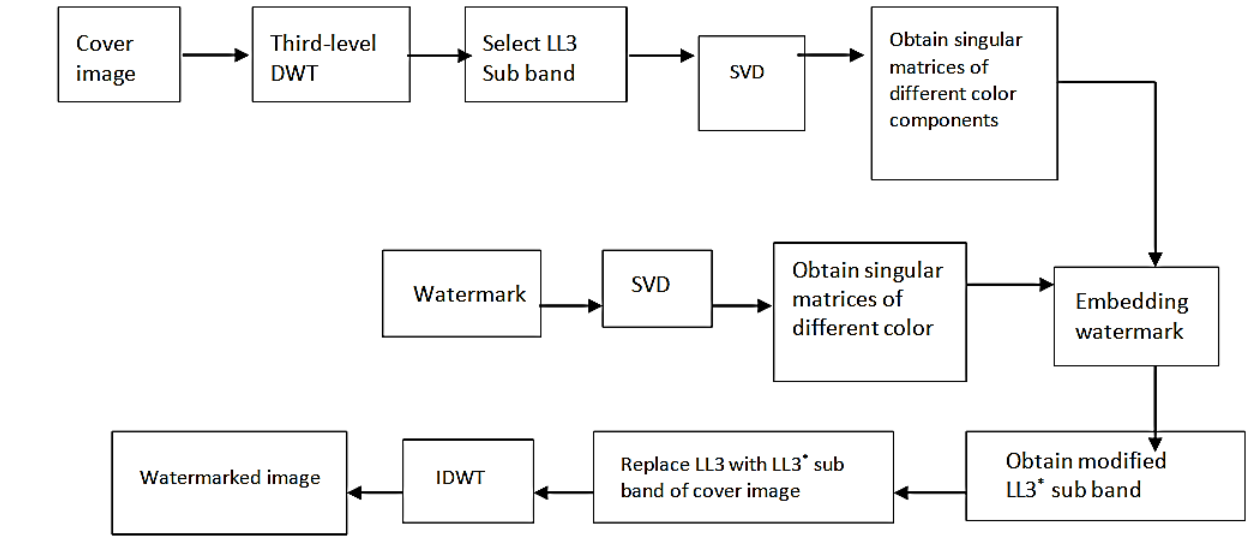
5.Obtain singular value of watermark image and singular value of LL3 subband of watermark image and cover image.

$S_{wi}^{*}=(S_{wati}- S_{ci})/k$

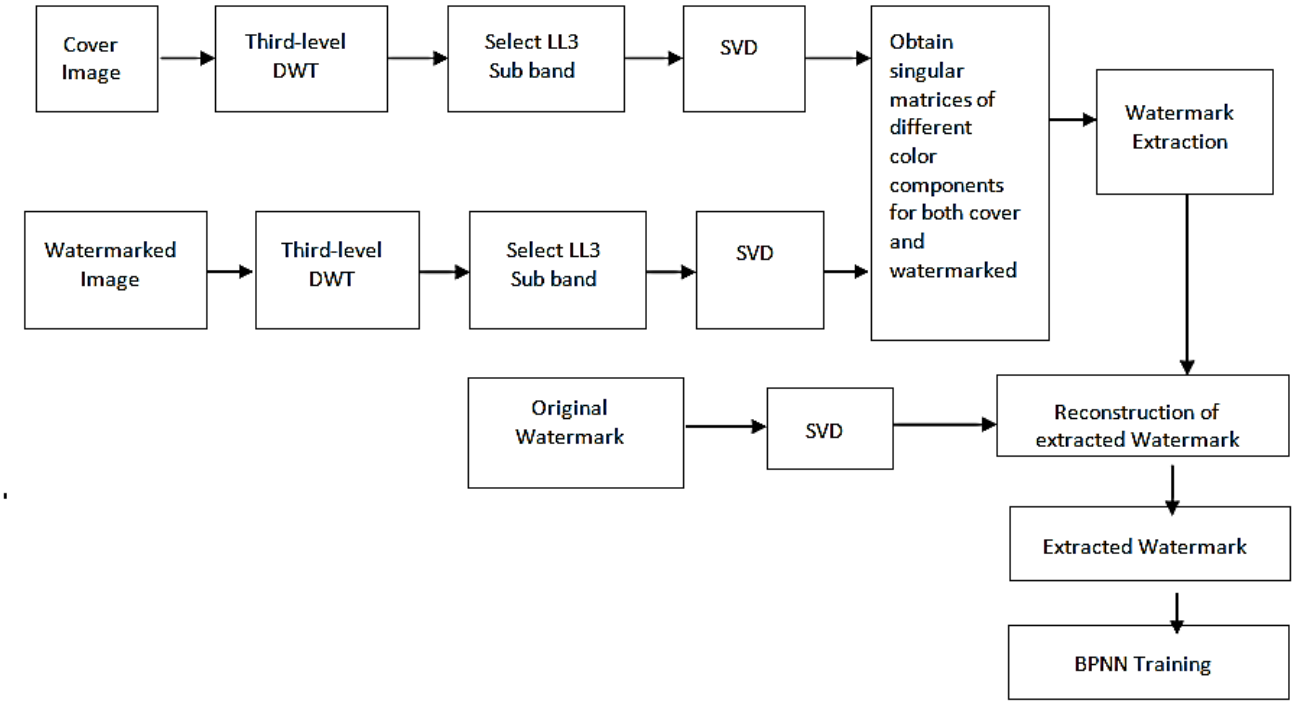
6. Obtain extracted watermark using this equation.

Aewi=Uwi* Swi* * VwiT

7. BPNN is then applied to extracted watermark to remove noise and interferences in order to improve its robustness.



(a)



(b)

Figure 3.1: (a) Watermark embedding and (b) Watermark extraction method

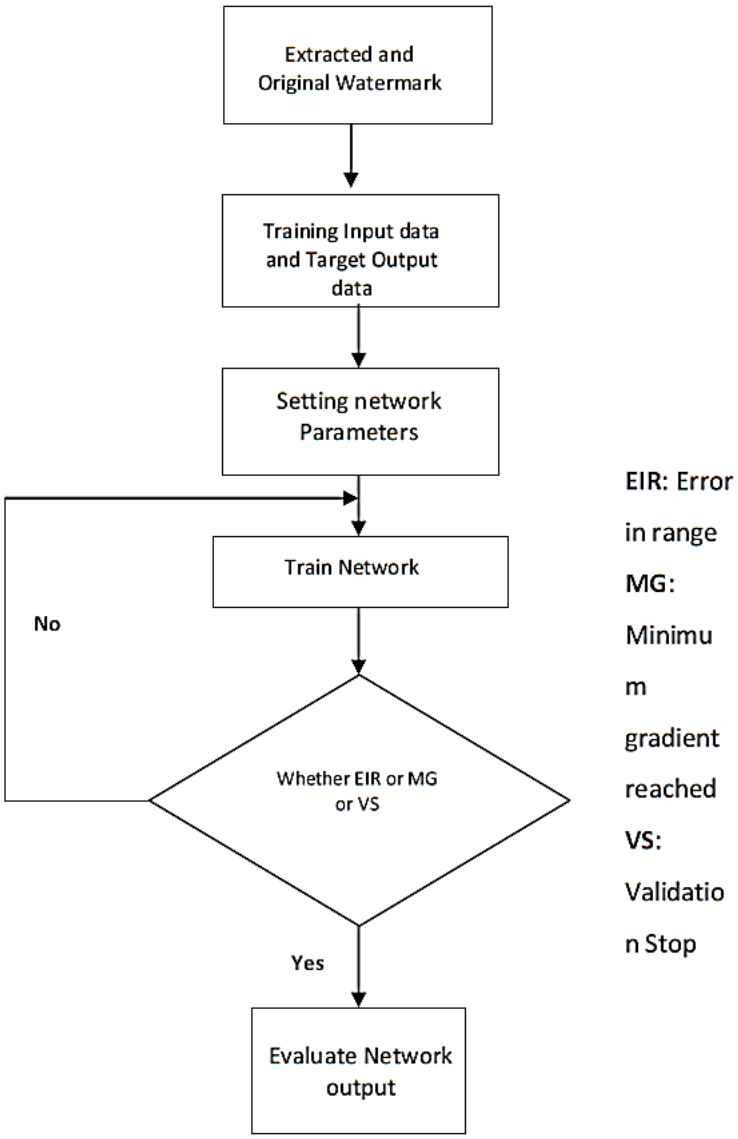


Figure 3.2: BPNN Training method

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding". IBM Systems Journal, Vol. 35, No 3.4, pp. 313-336, 1996.

[2] Provos, Niels, and Peter Honeyman, "Hide and seek: An introduction to steganography." Security & Privacy, IEEE, Vol. 1, No. 3, pp. 32-44, 2003.

[3] A. Cheddad, J. Condell, K. Curran and P. McKevitt, "Digital Image Steganography: Survey and Analyses of Current Methods". Signal Processing, Elsevier, Vol. 90, No. 3, pp. 727- 752, 2010.

[4] P. Singh and R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks". International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, No. 9, pp. 165-175, 2013.

[5] Amit Kumar Singh, Mayank Dave, and Anand Mohan, "Multilevel Encrypted Text Watermarking on Medical Images Using Spread-Spectrum in DWT Domain". Wireless Personal Communications, pp.1-18, 2015.

[6] W. Zhicheng, L. Hao, Dai Jufeng and W. Sashuang, "Image watermarking based on Genetic algorithm". IEEE International Conference on Multimedia and Expo, ICME, pp. 1117-1120, 2006.

[7] V. Aslantas, A. L. Dogan and Serkan Ozturk, "DWT-SVD based image watermarking using Particle Swarm Optimizer". IEEE International Conference on Multimedia and Expo, ICME, pp. 241-244, 2008.