Robust Digital Image Watermarking Using Glowworm Optimization and Neural Network

Chet Ram, Yogesh Kumar
Institute of Engineering and Technology Bhaddal, Ropar, Punjab

***Abstract*—** Digital Watermarking has been recognized as very vast research field to handle the challenges occurred during distribution of digital content over the network or internet. The digital content may be misused by unauthorized person or its copyright may be illegally claimed by someone who is not actually involved in creation of this digital content. So it is highly required to overcome these issues to protect the digital contents from unauthorized persons. Digital Watermarking techniques are very useful in this regard. In this technique a secret message is embedded into the actual digital content imperceptibly. The embedded secret message is called as ‘Watermark’. The watermark may be a company’s logo, some text, author’s serial number, and images of some special importance or a label. It could be further used for different applications such as copyright protection, authentication, and temper detection. In the paper, the Discrete Wavelet Transform (DWT) has been applied for image segmentation. Optimization of segmented image is achieved through Glow-worm Swarm optimization algorithm and lastly Advanced Encryption System (AES) is used to meet security requirements of watermarked image. The proposed method of digital watermarking improved the performance, efficiency and security as compared with existing methods. The results are also analyzed on the basis of performance parameters.

***Keywords*—** *Discrete Wavelet Transform; Advanced Encryption System; Glow-worm Swarm optimization; PSNR; MSE.*

I. INTRODUCTION

In present day a huge amount of data is embedded on digital media or distributed over the internet. These types of data include images, videos, audios or simply text. These data are transmitted in a digital format and can be easily copied without loss of quality. Thus the protection of intellectual property rights has become increasingly important. Information is stored in digital format because it is easy to reproduce, retransmit and manipulate the data. This will facilitate to a pirate either to remove a watermark and violate a copyright or to cast the same watermark after altering the data to forge the proof of authenticity [4]. The design of techniques for preserving the ownership of digital information is in the basis of the development of future multimedia services. In addition to Digital watermarking, the general idea of hiding some information in digital content has a wider class of applications that go beyond copyright protection and authentication. The techniques involved in such applications are collectively referred to as information hiding. For example, an image printed on a document could be annotated by information that could lead a user to its high resolution version. Metadata provides additional information about an image. Although metadata can also be stored in the file header of a digital image, this approach has many limitations. Usually, when a file is transformed to another format (e.g., from TIFF to JPEG or to bmp), the metadata is lost. Similarly, cropping or any other form of image manipulation destroys the metadata. Finally, the metadata can only be attached to an image as long as the image exists in the digital form and is lost once the image is printed. Information hiding allows the metadata to travel with the image regardless of the file format and image state [1].

II. DIGITAL WATERMARKING

A. *Similarity Between Watermarking And Communication System*

Watermarking can be considered as communication of the watermark over a channel consisting of the original work to be watermarked. Both watermarking and communication models transmit data from an information (the watermark) to a destination (the user or another system).The typical model of communication consists of several blocks. In order to transmit the discrete symbols over a physical channel, a modulator transforms each symbol of the encoded sequence into a form suitable for transmission. During transmission over the channel, the transformed sequence is distorted by noise. The different forms of noise that can disturb the transmission are driven by the channel characteristics. On the receiver side, the demodulator processes the transmitted sequence and produces an output consisting of the counterpart of the encoded sequence. Corresponding to encoder, the channel decoder transforms the output of demodulator into a binary sequence which is an estimation of the sequence being transmitted. Besides the channel characteristics the transmission can be further classified according to the security it provides against active attacks trying to disable communication and against passive attacks trying to monitor the communication [1].

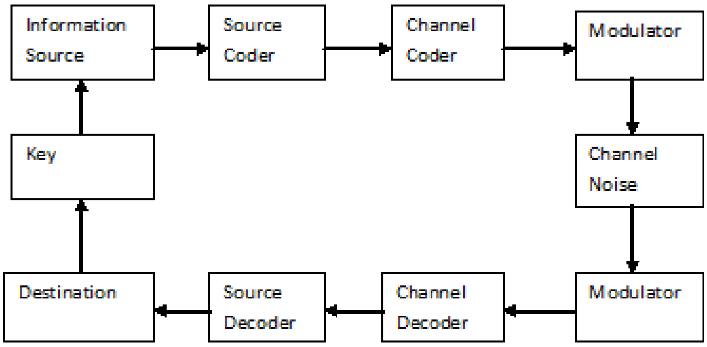


Fig 1.1 Basic Communication Systems [1]

B. Properties of Digtal Watermarking

To understand watermarking methods and determine their applications, one needs to know the properties of digital watermarks. Some fundamental properties are discussed below:

- **Imperceptibility**

This is the most important property of all watermarking schemes. The watermark must be embedded in the image in such a way that the resulting watermarked image is not visually distorted. This property is related to the robustness of the watermark and hence an optimal balance between imperceptibility and robustness must be achieved by the watermarking scheme [8].

- **Robustness**

This is another important property of a good watermarking scheme. Most schemes require that the watermark be recovered even if the watermarked image is being attacked and this attack may be intentional or unintentional. There are many types of attacks for a watermarking scheme including noise introduction, filtering, image compression, cropping, re-sizing, etc and the robustness to such attacks depends on the type of watermarking schemes and its accuracy. For example a fragile watermarking scheme does not require being robust against any attacks on the image as it is designed to confirm the occurrence of an attack [3].

- **Payload**

It is described as the total amount of watermark information bits that can be stored in the image. The amount of information bits to be embedded depends on the application. It is generally considered that the more the watermark bits (payload) in an image the higher the robustness of the watermark [8].

- **Security**

Another property of an ideal watermarking system is that it implements the use of Keys for the security (as in case of cryptography). It may also be a goal that the system utilizes an asymmetric key system such as in public / private key cryptographic systems. Although private key systems are fairly easy to implement in watermarking, asymmetric key pairs are generally not that much easy. The risk here is that embedded watermarking systems might have their private key discovered, corrupting security of the entire system [8]

III. TYPES OF DIGITAL WATERMARKS

The watermark which is embedded into the digital content can be of various types as shown in Figure 1.2

- **Visible And Invisible Watermark**

This type of watermark after embedding to host image is visible to the user that means this type of watermarks are visible to the outside world after watermarking. The watermark usually identifies the owner of the content and consists of a logo or seal of an organization. Whereas in case of invisible watermark, after embedding the watermark is invisible to user without degrading the image quality. Invisible watermark can be a logo or signature. Currently most researches focuses on invisible watermark rather than visible watermark [9].

- **Image Adaptive Watermark**

These types of watermarks are usually transform-based. They are locally adapt the strength of the watermark to the image content through perceptual models for human vision and were developed for image compression [5].

- **Fragile And Robust Watermark**

In case of fragile watermark if there is any small changes to image, the watermark distorted or broken easily. It is used to check the integrity of the image that means its intention is not to check robustness but to check the occurrence of attacks on image. On the other hand these types of watermarks are difficult to remove from watermarked image [9].

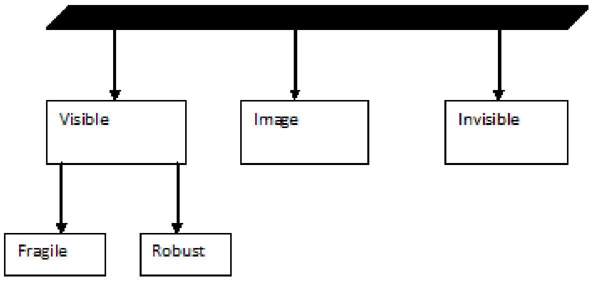


Fig 1.2 Types of Watermarks [9]

- **Non-Blind And Blind Watermarking**

In non-blind watermarking system, the original image is required while detecting the watermark. Whereas in blind watermarking original image is not required during detecting process. However blind watermarking is often less robust than non-blind watermarking [9].

- **Private Watermarking**

This type of watermarking systems are also called non-blind watermarking i.e. original image is required for detection process of watermark. The key used in detection process is secret one and not known to everyone [2].

- **Public Watermarking**

This technique is also known as blind watermarking. Here only a public key is needed for verification and a private key is required for embedding. During detection process the key is known to anyone. The knowledge of the public key does not help to compute the private key, it does not either allow removal of the mark nor it allows an attacker to forge a mark [9].

- **Asymmetric and Symmetric Watermarking**

In this type of watermarking technique the keys used for embedding and detecting the watermark are different. It should have the property that any user without being able to remove but can read the watermark [9].

- **Steganographic and Non-Steganographic Watermark**

In steganographic watermarking technique the content users are unaware of the presence of watermark. Whereas in non-steganographic technique the users are aware of the presence of watermark but also protects the images after they are resample. Steganographic watermarking is used in fingerprint applications while non-steganographic watermarking techniques can be used to prevent piracy [9].

A. *Advanced Encryption Standard (AES) Algorithm for Digital Watermarking*

Firstly an image is selected for transmission. This input image is then partitioned into wavelet sub-bands. Since there are HL, LH, HH and LL sub-bands, we choose only LL sub-band for encryption purpose because most of the image energy is concentrated in LL sub-band having lower frequency. The LL sub-band is encrypted by AES-128 (128 bit key) encryption algorithm. Only a part of the image is selected to for encryption instead of the entire image. This will reduce the computational time. There are 10 rounds in AES-128.This minimizes the number of if-else-then loops. Initially, input plaintext matrix is converted into state matrix by AES. State matrix is obtained by calculating hexadecimal value of input matrix which is given as input to the forthcoming steps of encryption. State matrix is obtained by rearranging the plain text matrix.

It iteratively loops through the steps as Addroundkey, Subbytes, Shiftrows, and Mixcolomns. The Addroundkey block operates in bitwise XOR of the state matrix and the round key matrix. The Subbytes block applies the S-box to one or more input bytes of input matrix. It performs the substitution function in which each byte of input matrix is replaced by the corresponding value in S-box. The block shiftrows cyclically permutes (shifts) the rows of state matrix to the left. It takes the output matrix from subbytes step, cyclically shift the rows and give its output to next step. Polynomial matrices are used in the mixcolumns function, both matrices have the size of 4 × 4 and every row is a cyclic permutation (right shift) of the previous row. The mixcolumns transformation computes the new state matrix S0 by left multiplying the current state matrix S by the polynomial matrix P. The input parameters for encryption process are: the substitution table S-box, the key schedule w, and the polynomial matrix [].

B. *Glowworm Swarm Optimization For Digital Watermarking*

Glow-worm swarm optimization exploits the collective nature of glow-worms. Glow-worms are a lightening bug whose brightness depends on a substance known as luciferin. The value of luciferin decides with which intensity a glow-worm will glow. Higher the value of luciferin, brighter the bug and lesser value lead to less light intensity with which the glowworm glows. Each glow-worm has its own sensor range and decision range. Sensor range determines the neighbor of glowworm and decision range determines which glow-worms can move towards it. There are two phases: movement phase and luciferin updating phase. The movement of glow-worm in the search space is such that they move towards the glow-worm that glows brighter than it and that resides in its circular sensor range. After that the decision range of each neighbor is checked to see whether the glow-worm that wants to move towards them resides in it or not. If multiple such neighbors exist, in whose decision range the glow-worm in question resides then probability is being calculated to find the neighbor for final movement. Luciferin updating phase updates the luciferin value of each glow-worm according to its current luciferin value and according to the goodness of the new position attained. The decision range of each glow-worm is also updated which is governed by current decision range and the number of neighbors found. Hence moving towards glowworm that has better luciferin value leads to an ultimate arrangement, that is optimized. In the paper the work has been proposed a novel feature selection algorithm for image steganalysis-Glow Worm Swarm Optimization. To the best of the insight, this is the first endeavor to utilize Glow-worm Swarm optimization with Extreme Learning machine (ELM) for choosing the diminished list of feature set for image steganalysis.[10]

1) *Feature Selection using Glow-worm Swarm Optimization Algorithm*

Glow-worm swarm optimization algorithm exploits the swarm intelligence nature of an insect known as “glow-worm” (fireflies). As the name says glow-worm are the lighting bug that are capable of emitting light at different intensities. The intensity of light with which a glow-worm glows depends on the amount of luciferin (a substance) emitted by the glowworm. Lesser the amount of luciferin lesser is the intensity of light with which glow-worm glows and vice-versa. Glowworm flies in their search space and move closer to glowworm that glows brighter than them. Each glow-worm has a circular sensor range (Rs) that describes its neighborhood. We have used Euclidian Distance to measure the distance between two glow-worms. When a glow-worm moves in the search space they consider only those glow-worms that tend to fall in its sensor range. Glow-worms moving outside its sensor range are not being considered. All those glow-worm in its sensor range that has higher luciferin value as compared to their own luciferin value are shortlisted as few of the final glow-worms for movement. Then each glow-worm is considered one by one and their decision range is being checked to verify whether the glow-worm that is trying to come closer to them resides in their decision range (Rd) or not. The decision range of a glow-worm resides within its circular sensor range ($0 < Rd \leq Rs$). Now if the glow-worm that is trying to move has several neighbor in whose decision range it resides, then it probabilistically move towards one of them. For each glow-worm i, the probability of moving towards a neighbor j is given by equation 4.1

$$p_j\ (t) = \frac{lj\ (t) - li(t)}{\sum_{k \in Ni(t)} lk(t) - lit)}$$

Equation – 4.1 [10]

where, $j \in Ni(t)$, $Ni(t) = \{ j : di,j(t) < ri\ d(t); li(t) < lj(t)\}$, t is the time index, di,j (t) represents the Euclidian Distance between glow-worms i and j at time t and li represents the luciferin value of the ith glow-worm . The neighbor with the highest probability is the best candidate for the movement and the glow-worm moves towards it. The luciferin value and hence the intensity with which a glow-worm glows is also updated. In the proposed feature selection algorithm using glow-worm swarm optimization, each glow-worm is considered to be an agent whose position is represented as bit string. Bit string of 1 and 0 represents the presence and absence of features. '1' signifies that the corresponding feature is present and '0' means the corresponding feature is absent.

2) Steps for the Algorithm

The main steps of the proposed algorithm are:

- **Initialization**

The agents (glow-worm) are initialized in this phase i.e. each agent's position is randomly assigned with bit string that has random number of features on. Other parameters used are:

➢ Circular Sensor Range, of some percentage of number of features, N.

➢ Randomly initialised decision range, rd which varies between 0 to rs.

➢ Luciferin decay constant, ρ and enhancement constant, ϒ whose value varies between 0 to 1 are also set in this phase.

- **Luciferin Updation Phase:**

In this phase, the luciferin value is updated for each glow-worm. The luciferin is updated by the formula:

$$\mathbf{lj\ (t+1) = (\ 1 - \rho\ )\ lj\ (t) + \gamma\ Jj\ (t+1)}$$

Equation- 4.2

This equation is governed by two parameters "Luciferin Enhancement Constant" (ϒ) and "Luciferin Decay Constant" (ρ) . The decay constant specifies by what fraction the new luciferin value should be dependent on the old value and the enhancement constant specifies by what percentage the new luciferin value should depend on the classifier accuracy is obtained after the glow-worm reaches its new position. The value of both decay and enhancement lies between 0 and 1. Jj(t) represents the value of the objective function at agent j's location at time t and li represents the luciferin value of the ith glow-worm [11].

- **Movement Phase:**

This phase includes several steps and all steps are followed for each glow-worm.

➢ All the neighbours of the glow-worm are determined that have luciferin value greater than their own luciferin value. The neighbours are found using Euclidian Distance.

➢ For each neighbours their decision range is checked to see whether the glow-worm who wants to move towards them lie in their decision range not.

➢ If multiple such neighbours exist then probability is calculated for each neighbours as specified in equation (eq 4.1.1) above and the glow-worm moves towards the glow-worm with highest probability.

➢ Since we are dealing with bit strings hence the movement of a glow-worm towards other glow-worm is in form of bit flips. The number of bits to be flipped is calculated by multiplying the step size s (a random variable between 0 and 1) with the Euclidian distance between the two glow-worms. Then bit-wise matching of feature bit string of both glow-worms is done. If corresponding bits are not same, the bit in the string corresponding to the glow-worm that is moving is flipped to match it to the bit of the string corresponding to glow-worm towards which it is moving. This is done until required number of bits is flipped. This marks the end of glow-worm movement and the glow-worm reaches its new position [10].

1. After that the decision range (rd) for each glow-worm is updated according to equation:\

$$\mathbf{rd\ (t+1) = \min\{\ rs,\ \max\ \{\ 0,\ rd\ (t) + \beta\ (\ nt - |\ Ni(t)\ |\ )\ \}\ \}}$$

Equation-4.3 [10]

Here nt is a parameter that controls the number of neighbours a glow-worm has in each iteration and β is a constant.

2. Both the luciferin updating and the movement phase are repeated a predefined number of times.
3. Now to get the solution, the best glow-worm (the bit string with the maximum classifier's accuracy) is chosen among all the glow-worms.

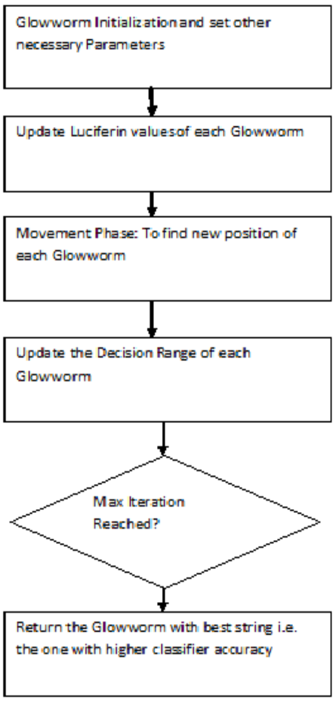

Glowworm Initialization and set other necessary Parameters
Update Luciferin values of each Glowworm
Movement Phase: To find new position of each Glowworm
Update the Decision Range of each Glowworm
Max Iteration Reached?
Return the Glowworm with best string i.e. the one with higher classifier accuracy

Fig 1.3 Glow-worm Algorithms. [10]

The Glowworm Optimization is shown in the fig given below-

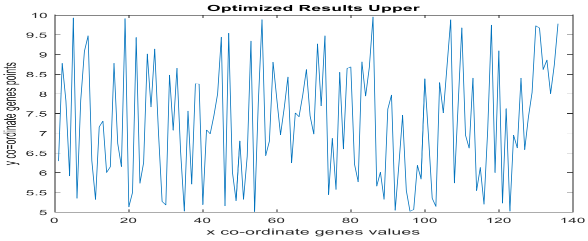
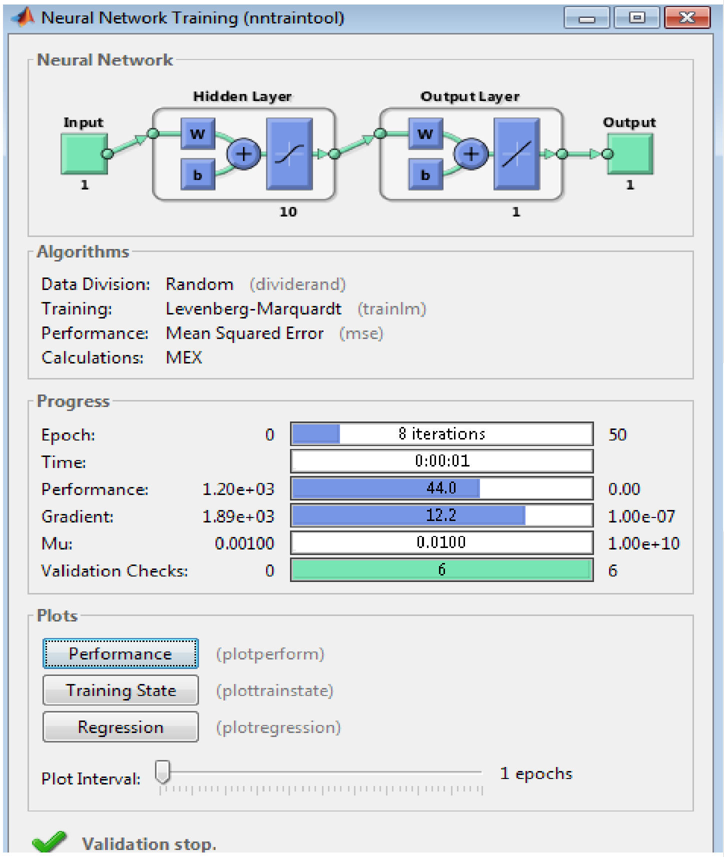


Fig 1.4 [10]

C. *Neural Network*

Neural Network is one of the most important steps for training and it has fast reaction time and response time which will train the system in efficient manner. The other advantages are:

- Moderately easy to practice
- Can estimated any function, irrespective to its linearity
- Countless for complex difficulties like pattern recognition [12].



Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

```
Epoch:                 0   8 iterations   50
Time:                      0:00:01
Performance:    1.20e+03   44.0           0.00
Gradient:       1.89e+03   12.2           1.00e-07
Mu:              0.00100   0.0100         1.00e+10
Validation Checks:     0   6              6
```

Plots

Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)

Plot Interval: 1 epochs

✓ Validation stop.

Fig 1.5 Neural Networks [12]

IV. RESULTS AND CONCLUSION

The techniques have been developed to protect the ownership information of the digital content by watermarking on gray and color digital images integrating the concept of digital watermarking and image processing.

A watermarking is the process of identifying image that looks as numerous shades of brightness of darkness used for the security in image processing. Digital watermarking using image processing is a type of marking embedded in a noisy area like as in video or image data. It is characteristically used to classify tenure of the patent of such data. It is the approach of hiding digital data in an image. It may be recycled to confirm the genuineness or truthfulness of the data or to show the individuality.

The hybridization approach is applied which is using discrete wavelet transform for the hybridization with neural and Advance encryption scheme for the security in the testing phase.

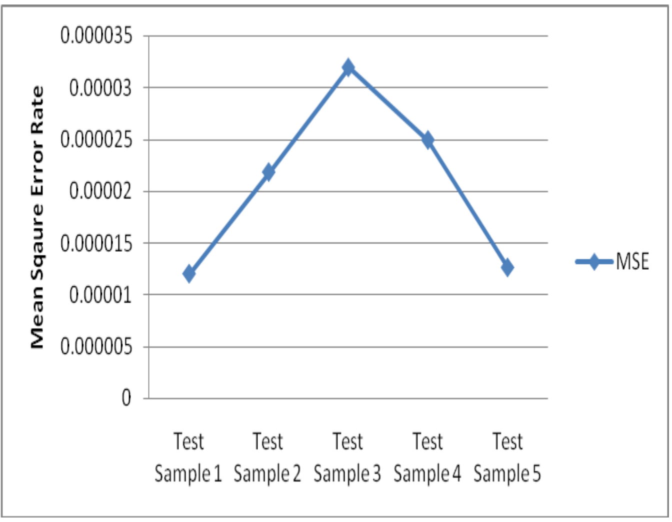


Fig 1.6 Mean Square Error rate [12]

The figure 1.6 shows the Mean Square Error rate comparison on various test samples of the images and shows that the system is well suited to achieve less error rate probabilities.

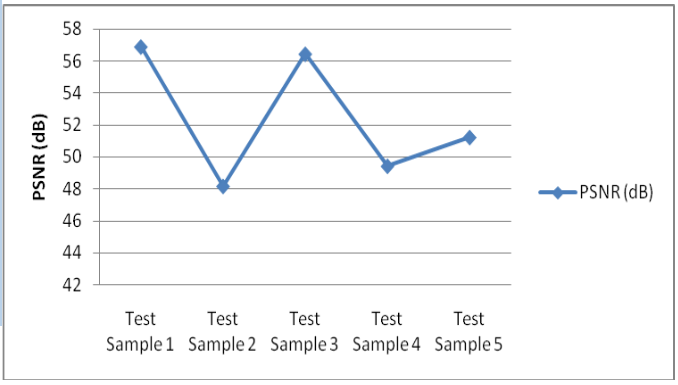


Fig 1.7 Peak Signal to noise Ratio [12]

The figure 1.7 shows the peak signal to noise ratio which must be high for the high efficient watermarking system and shows that the proposed system is able to achieve high peak signal to noise ratio which shows the robustness of the system in harsh environments

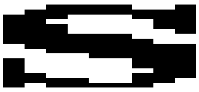


Fig 1.8 Watermark image [12]

The above figure shows the image which is to be watermarked and embedded in the original image and which must be extracted at the end after the embedding process

The mean square error rate must be low and peak signal to noise ratio must be high for the high efficiency of the system. If the PSNR is high and MSE is low it means the system is well suited for the high efficiency of the system with less error probabilities.

Table 1: Performance Comparison [12]

Parameters	MSE	PSNR (dB)
Test Sample 1	0.000012	56.9
Test Sample 2	0.0000218	48.1692
Test Sample 3	0.0000319	56.45
Test Sample 4	0.0000249	49.43
Test Sample 5	0.0000126	51.23

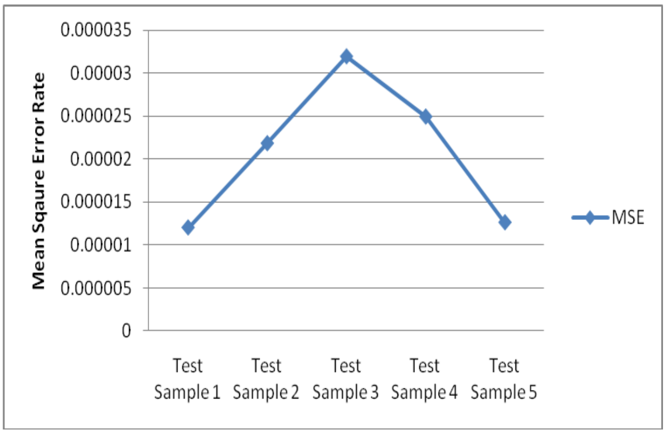


Fig 1.9 MSE comparison [12]

The figure 1.9 shows the Mean Square Error rate comparison on various test samples of the images and shows that the proposed system is well suited to achieve less error rate probabilities

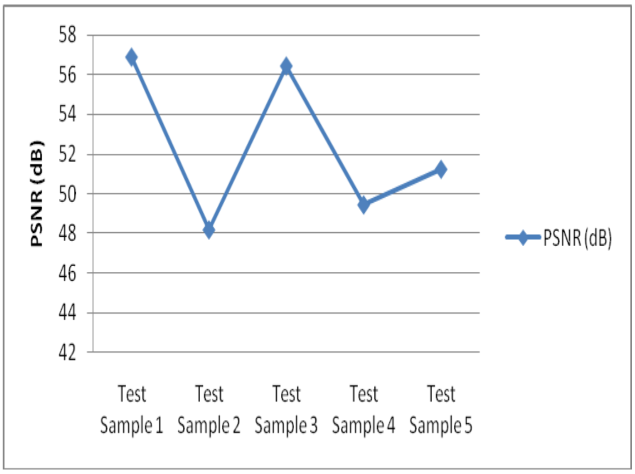


Fig 1.10 Peak Signal to noise Ratio [12]

The figure 1.10 shows the peak signal to noise ratio which must be high for the high efficient watermarking system and shows that the proposed system is able to achieve high peak signal to noise ratio which shows the robustness of the system in harsh environments

Table 2: Error Rate [12]

Parameter	Base	Proposed
Error Rate	0.5	0.000012

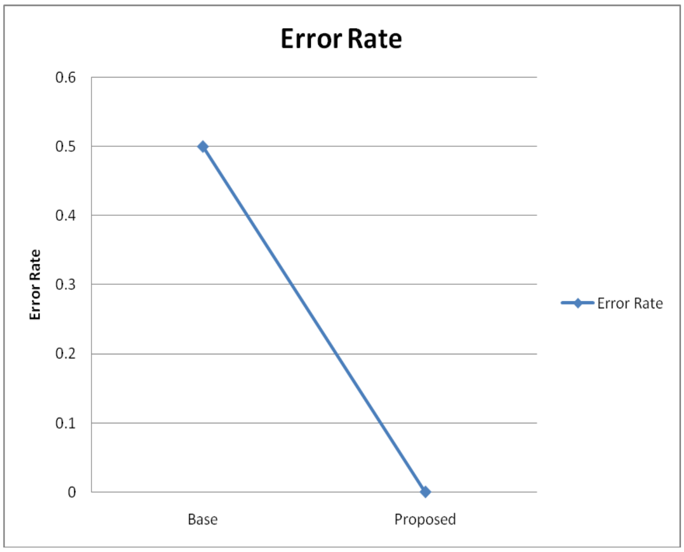


Fig.1.11 Error Rate [12]

The figure 1.11 shows the comparison between the base and proposed approach in which it shows that the proposed approach is well suited to achieve low error rates than the others base solutions and shows that the proposed system is well suited for image watermarking

V. CONCLUSION AND FUTURE SCOPE

Digital Watermarking can protect the copyrights of an image from various illegal and unauthorized ownerships. It also deals with security of an image on the communication network. The Digital Watermarking technique proposed in this research work is comparatively much better than the special- domain watermarking. The Watermarking technique here is very suitable against various attacks like noising and sharpening. In the present proposed work the overall system is dealt with Discrete Wavelet Transform (DWT) for decomposition purpose. The segmentation is done by applying low pass and high pass filters. Optimization is achieved by applying Glow-worm Swarm algorithms; and lastly Neural Network is used for training the system. The AES (Advanced Encryption Scheme) is used to protect the system from various spoofing attacks which means the security measure is achieved by applying AES algorithms. Hence it is clear from the evaluated results in the proposed system that high ratio of signal to noise is achieved with lower error rates.

The Discrete Wavelet Transform technique can be used here for watermarking of an image data file. So we can conclude that the digital watermarking is a significant approach for protection of copyrights on digital properties. Different watermarking techniques are used for various types of requirements. However, it is difficult to satisfy all the requirements at the same time. So, PSNR (Peak-Signal to Noise Ratio) can be used to compare the noise ratios of different sample used for research work. There may be a scope of future study in the present study. Future study can be implemented by analysis of watermarking on different machine learning algorithms and making a comparison of signal to noise ratio on different platforms. Secondly, we can attempt to do the research work on focusing on attack scenarios and evaluate the performance of the entire system.

VI. REFERENCES

[1] Amit Kumar Rathore and Anurag Jain, "A New Visual Cryptography Approach using Mosaic and Spread Spectrum Watermarking", International Jthenal of Computer Applications (0975 – 8887) in 2017, Volume 165, No.10.

[2] Anirban Patra, Arijit Saha and Ajay Kumar Chakraborty, "A Simple Approach to Watermarking of Multiple Grayscale Images using Alpha Blending", International Research Jthenal of Engineering and Technology (IRJET) in 2017, Volume: 04 Issue: 03.

[3] Baowei Wang, Jianwei Su, Youdong Zhang, Biqiang Wang, Jian Shen, Qun Ding and Xingming Sun, " A Copyright Protection Method for Wireless Sensor Networks Based on Digital Watermarking", International Jthenal of Hybrid Information Technology in 2015, Vol.8, No.6, pp.257-268.

[4] Gaurav Gupta , Amit Mahesh Joshi and Kanika Sharma, " An Efficient Robust Image Watermarking based on AC Prediction Technique using DTC Technique", ICTACT Jthenal On image and Video Processing in 2015, VOLUME: 06, ISSUE: 01

[5] Gaurav Tiwari, "A Review on Robust Watermarking with its Applications and Comparative Analysis", International Jthenal of Signal Processing, Image Processing and Pattern Recognition in 2015, Vol.8, pp.85-90.

[6] Jayashree S. Pillai1 and Padma Theagarajan, "Semi Fragile Watermarking for Content based Image Authentication and Recovery in the DWT-DCT domains in 2015".