A Robust Approach of Digital Watermarking using AES and Genetic methods

Rahul Mahendru, Er. Saranjeet Singh
Galaxy Global Group of Institutions, Ambala, Hariana, India

***Abstract*—** Digital watermarking has become a promising research area to face the challenges created by the rapid growth in distribution of digital content over the internet. To prevents misuse of this data Digital watermarking techniques are very useful in which a Secret message called as a watermarks which can be a logo or label is embedded into multimedia data imperceptibly which would be then used for various applications like copyright protection, authentication, and tamper detection etc. Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author's serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. The basic principles of digital watermarking technology means that the digital watermark information has a certain significance in the premise does not affect the value of the embedded covertly through a different approach to digital data processing work to become part of the work cannot be separated from the carrier. In the research, we have implemented the DWT for segmentation of image, Genetic for optimization for segmented image and AES is used for providing the security to watermarked image. The proposed method of watermarking improved the performance, security and efficiency as compared to existing methods. The results are also analyzed on the basis of performance parameters.

***Keywords*—** *Steganography; Digital watermarking copyyright, AES, DWT; Stego image PSNR, MSE.*

I. INTRODUCTION

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark .For visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals. Digital documents i.e. documents created in digital media are having certain Advantages like-

- Efficient data storage, duplication, manipulation and transmission.
- Copying without loss. Such digital documents consist of images, audio clips and videos. But due to some delimits of digital documents, they become inefficient to use. These delimits are as follows
- Illegal copying
- Falsification(duplication)
- No copyright protection
- No ownership identification

The large use of networked multimedia system has created the need of "Copyright Protection" for different digital medium as images, audio clips, videos etc. The term "Copyright Protection" involves the authentication of ownership and identification of illegal copies of digital media. Though digital media provides various efficient facilities like distribution, reproduction and manipulation of images, audio clips and videos, they increase illegal copying of digital media. The solution for this problem is to add the visible or invisible structure to digital media which is to be protected from copyright. These structures are known as "Digital Watermarks" and the process of adding digital watermarks to digital media is known as "Digital Watermarking". Digital watermarking is created by inserting a digital signal or pattern into digital content. Digital watermarking is nothing but process of conveying information by imperceptibly embedding it into digital media. The purpose of embedding the information depends upon application and need of user of digital media.

a) STEGANOGRAPHY VS WATERMARKING

Watermarking is the subset of Stegnography. In Stegnography, data which is hidden has no relationship with the cover medium and the requirement from such a system is that no suspicion should arise that a medium is carrying any hidden data. In watermarking, unlike stegnography, the data which is hidden has relationship with the cover medium

data. Data hidden is the ownership data of the cover medium and there is no issue like suspecting that a particular medium is carrying some copyright data.As the purpose of stegnography is to have a covert communication between two parties i.e.existence of the communication is unknown to a possible attacker, and a successful attack shall detect the existence of this communication. On the contrary, watermarking, as opposed to stegnography, requires a system to be robust against possible attacks.

b) CRYPTOGRAPHY VS. WATERMARKING

Cryptography can be defined as the processing of information into an unintelligible form known as encryption, for the purpose of secure transmission. Through the use of a "key",the receiver can decode the encrypted message (the process known as decryption) to retrieve.So, *cryptography* is about protecting the contents of the message. Butas soon as the data is decrypted, all the in-built security and data is ready to use.Cryptography "scrambles" a message so that it cannot be understood by unauthorized user.This does not happen in watermarking. Neither the cover medium nor the copyright data changes its meaning. Rather, copyright data is hidden to give the ownership information ofthe medium in which it is hidden.

c) DIGITAL SIGNATURE VS. WATERMARKING

Digital signatures, like written signatures, are used to provide authentication of the associated input, usually called a "message". Digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else,and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital signature is a part from the protected message, whereas a digital watermark is inside a multimedia message. Both, digital signature and watermarking protect integrity and authenticity of a document. Digital signature system is vulnerable to distortion but a watermark system has to tolerate a limited distortion level.So, to conclude, *Watermarking is adding"ownership" information in multimedia contents to prove the authenticity*. This technology embeds a data, an unperceivable digital code,namely the watermark, carrying information about the copyright status of the work to be protected. Continuous efforts are being made to device efficient watermarking schema but techniques proposed so far do not seem to be robust to all possible attacks and multimedia data processing operations. The sudden increase in watermarking interest is most likely dueto the increase in concern over IPR. Today, digital data security covers such topics as access control, authentication, and copyright protection for still images, audio, video, and multimedia products. A pirate tries either to remove a watermark to violate a copyright or to cast the same watermark, after altering the data, to forge the proof of authenticity. Generally,the watermarking of still images, video, and audio demonstrate certain common fundamental concepts.

II. PREVIOUS WORK

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden "mark" that is imprinted into the image. In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from digital watermarking.

Maninder Kaur et al.[1] proposed method presents a technique which is based on combination of spatial domain technique and frequency domain techniques. Discrete wavelet transform, singular value decomposition and least significant bit techniques are combined to provide robustness to the watermark image as well as to improve the quality of obtained watermarked image. In the research, a new combined digital image watermarking technique is presented and from the results of performance metrics it shows that the proposed method of watermarking is efficient based on the quality of the watermarked image obtained and recovered watermark after different attacks. This proposed method provides better image quality and better watermark extraction than robust digital watermarking scheme based on RDWT-SVD. It will provide security to the digital documents and will help to provide copyrights to original owner of digital contents. Further work can be done to implement this scheme for colored images and to check its robustness against geometric attacks.

Zhu Yuefeng et al.[3]introduced to the digital watermarking technology. Simulation study of a digital image watermarking algorithm based on DCT transform and Arnold transform, the algorithm's imperceptibility, robustness and security are analyzed, the algorithm for embedding process. In view of dual watermarking algorithm for dual two value image watermarking, the watermark information there is a gray image watermarking in the expression is obviously insufficient. The proposed embedded in the carrier image on the dual watermark includes a two watermark image and a gray image watermarking algorithm, the persuasive power while

maintaining the original two values of the watermark robustness at the same time, improve the watermark information. In order to balance the robustness and invisibility of watermarking algorithm, this paper analyzes the embedding position and strategy of transform domain algorithms, the DC coefficient in the carrier image is divided into blocks of DCT spectrum and spectrum on the combination of DWT coefficient method and the advantage of embedded dual watermarking, and use the NEC characteristic of the algorithm is improved adaptive based on the embedded mode.

Samira Lagzian et al. [12] proposed a new method for non-blind image watermarking that is robust against affine transformation and ordinary image manipulation is presented. The suggested method presents a watermarking scheme based on redundant discrete wavelet transform and Singular Value Decomposition. After applying RDWT to both cover and watermark images, we apply SVD to the LL sub bands of them. We then modify singular values of the cover image using singular values of the visual watermark. The advantage of the proposed technique is its robustness against most common attacks. Analysis and experimental results show higher performance of the proposed method in comparison with the DWT-SVD method.

Ahmidi N. et al. [15] discussed focusing on visually meaningful color image watermarks; we construct a new digital watermarking scheme based on the Discrete Cosine transformation. The proposed method uses the sensitivity of human eyes to adaptively embed a watermark in a color image. In addition, to prevent tampering or unauthorized access, a new watermark permutation function is proposed, which causes a structural noise over the extracted watermark. Also, we have proposed a procedure to eliminate this noise to decrease false positives and false negatives in the extracted watermark. The experimental results show that embedding the color watermark adapted to the original image produces the most imperceptible and the most robust watermarked image under geometric and valumetric attacks.

III. PROBLEM FORMULATION

Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. The system consists of two modules which are watermark embedding module and watermark detection and extraction module. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. With a lot of information available on various search engines, to protect the ownership of information is a crucial area of research. In the research, the neural network is used for training and testing the image of watermarking and AES method is used for provide the security for watermarked image. Genetic method is also used to optimized the segmented pixels.The ultimate objective of the research is to prove that the propose method of watermarking is efficient based on the quality of the watermarked images. The proposed method will also provides better image quality, more security and better watermark extraction than the existing methods.

IV. RESEARCH OBJECTIVES

A Watermark is a form, image or text that is impressed on

to paper, which provide evidence of its authenticity.

Digital Watermarking is an extension of this concept in the digital world. The objectives of the research work are:

- To study and analyze the existing techniques for watermarking.
- To use the neural network for training the images.
- To apply the DWT for the segmentation of the image.
- To apply the Genetic optimization method to improve the segmented pixels.
- To finally apply the AES method of security to test the watermarked image.
- To compare and analyze the existing and propose techniques on the bases of performance metrics such as PSNR and MSE.

V. RESULT & DISCUSSION

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 or we can say hidden information. It may be recycled to confirm the genuineness or truthfulness of the data or to show the individuality. In the paper, we have used an appropriate hybridization of the approaches in which we have used discrete wavelet transform for the hybridization

with neural and Advance encryption scheme for the security in the testing phase. Below are the results and discussions of the proposed approach left side is the panel of operations and in the main sub windows it is given various plots on which the uploaded figures and operations are shown. The graphical user interface is made using user interface controls using push buttons, static texts, labels and edit texts.

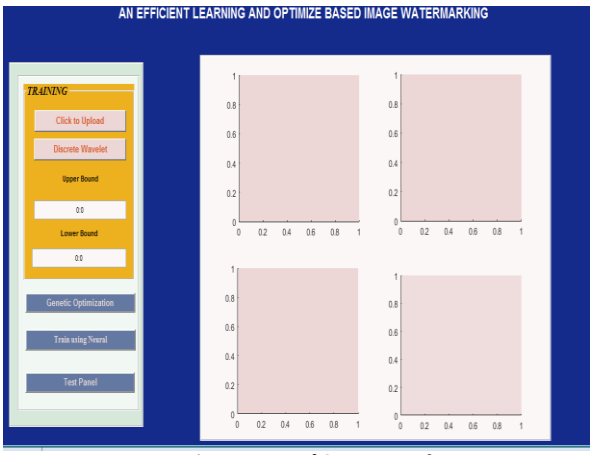

Fig 1: Types of Steganography

Fig. 2: Testing result panel

The above figure shows the result testing panel in which the Watermarked image sample is shown. The left side shows the panel in which embedding and extraction process is done after clicking on the embedding and extraction button. It is also showed that the performance is evaluated using mean square error rate and peak signal to noise ratio. 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 our system is well suited for the high efficiency of the system with less error probabilities.

VI. OUTPUT TABLES AND GRAPHS

Table 1: output table

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

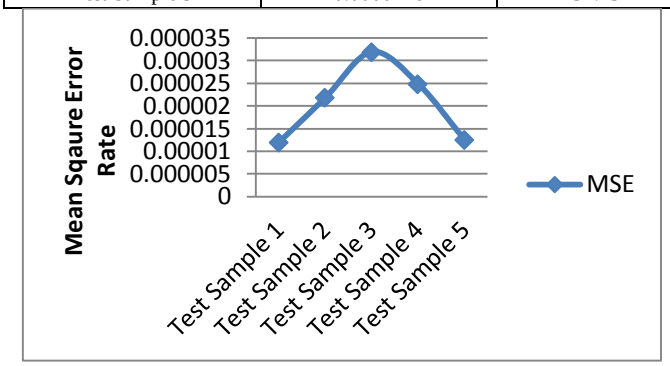

Fig. 3: MSE comparison

The figure 5.10 shows the Mean Square Error rate comparison on various test samples of the images and shows that our proposed system is well suited to achieve less error rate probabilities

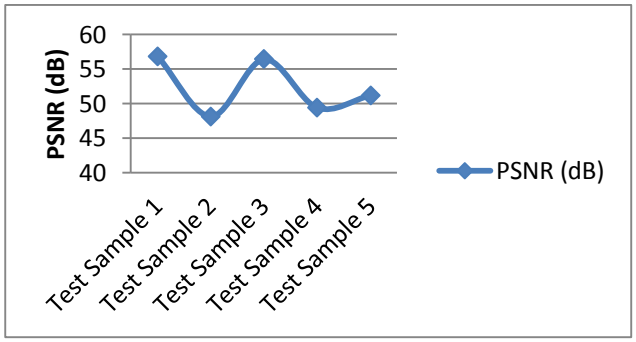

Fig. 4: Peak Signal to noise Ratio

The figure 5.11 shows the peak signal to noise ratio which must be high for the high efficient watermarking system and shows that our proposed system is able to achieve high peak signal to noise ratio which shows the robustness of our system in harsh environments

Table 2: Comparison Table

Parameter	Base	Proposed
Error Rate	0.5	0.000012

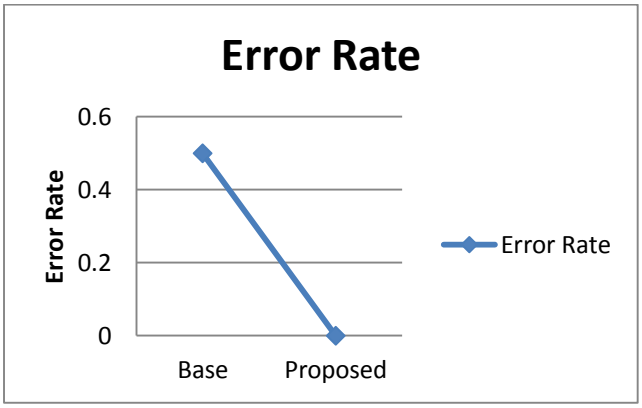

Fig. 4: Error Rate

The figure 5.12 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 base and shows that our proposed system is well suited for image watermarking.

VII. CONCLUSION AND FUTURE WORK

Digital Image Watermarking can defend image from unsanctioned or unauthorized activities, various distortions, copyright etc. The proposed approach based digital watermarking is relatively much healthier than the spatial domain watermarking which can survive contrary to the various attacks like noising, sharpening. In this research work the system deals with the DWT for decomposition, segmentation in terms of low pass and high pass filters and then genetic algorithm is used for the optimization and neural is used for the training of the system. Also In this research work security approach is applied using advance encryption scheme to secure the system from the various spoofing attacks. So from the evaluated results we can noticed that our proposed system is able to achieve high signal to noise ratio with less error rates. The future work can be implemented using comparative analysis based on different machine learning algorithms and also we can work on the implementation of the attack scenarios and can evaluate the performance of the whole system

VIII. REFERENCES

[1]. Maninder Kaur and NirvairNeeru, " Digital Image Watermarking using New Combined Technique" in the International Journal of Computer Applications (0975 – 8887) Volume 145 – No.2, July 2016.

[2]. SmitaPandey and Rohit Gupta, "A Comparative Analysis on Digital Watermarking with Techniques and Attacks" in the International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016.

[3]. Zhu Yuefeng and Lin Li, "Digital Image Watermarking Algorithms Based on dual Transform Domain and Self-Recovery" International Journal on Smart Sensing and Intelligent Systems Vol. 8, No. 1, March 2015.

[4]. Sumedh P. Ingale 1 and Dr.C.A.Dhote, "A Survey Of Digital Watermarking Techniques" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 2 February 2015.

[5]. DeeptiShukla and NirupamaTiwari, "Survey on Digital Watermarking Techniques" in the International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.9 (2015), pp.121-126.

[6]. Ruchika Patel and Parth Bhatt, " A Review Paper on Digital Watermarking and its Techniques" in the International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 1, January 2015.

[7]. Radhika v. Totla and K.S.Bapat, "comparative analysis of Watermarking in Digital Images using DCT & DWT" International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.

[8]. Prabhishek Singh and R S Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" in the International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.

[9]. Shraddha S. Katariya, "Digital Watermarking: Review" in the International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 2, February 2012.

[10]. ManjitThapa, Dr. Sandeep Kumar Sood and A.PMeenakshi Sharma, " Digital Image Watermarking Technique Based on Different Attacks" in the *International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011*.

[11]. Nidhi Rani "Digital Watermarking" in the Global Journal of Computer Science and Technology Graphics & Vision Volume 12 Issue 13 Version 1.0 Year 2012.

[12]. SamiraLagzian, Mohsen Soryani and MahmoodFathy,"A New Robust Watermarking Scheme Based on RDWT–SVD", International Journal of Intelligent Information Processing, 2011, Vol. 2 (1).

[13]. V Santhi and Dr. ArunkumarThangavelu, "DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Spaces", International Journal of Computer Theory and Engineering, 2009, Volume 1 (4), pp: 424 - 429.

[14]. C.C. Chang, C.C. Lin, Y.S. Hu, "An SVD oriented watermark embedding scheme with highqualities for the restored images", International Journal of Innovative Computing, Information andControl (ICIC), vol. 3, no. 3, pp. 609-620.

[15]. Ahmidi N., Safa R., *"A Novel DCT-based Approach for Secure Color ImageWatermarking"*, Proc. Int. Conf. on Information Technology: Coding andComputing (ITCC'04), page 709, IEEE, 2004.