Improve the Quality of the Image Watermarking Using AES Encryption Technique

Ashminder Kaur[1], Ms. Lofty Sahi[2]
[1]*M.Tech Scholar,* [2]*Assistant Professor*
Chandigarh Engineering College, Landran, Punjab, India

Abstract - Image watermarking includes extra information about image in the form of image or text. In this paper defines a protected multi-level watermarking scenario in which the encrypted text acts as a watermark. The procedure is created on the protected supper range or frequency domain method for numeral images in discrete wavelet transformation. Latent Application of the proposed watermarking technique is successfully demonstrated for embedding various watermarking techniques in the text/image format at different sub-categories decomposition levels depending upon their performance requirements. In the embedding process, we can apply the DWT decays an input into two components like lower bound and upper bound. An encryption using advanced encryption standard is a symmetric encryption calculation for encrypt the images. Encryption of a block of the message takes place in 128 blocks. From the input key are generated one for each round. To reduce the secrete message then classify the network using BPNN. Watermarking differs from the cryptography such that cryptography hides the information of underground message, whereas. Digital watermarking is about hiding the message in broadcasting successfully. In this paper defined that the text watermarking with image, used the encryption algorithm using Advanced Encryption Standard, Classification using BPNN and evaluate the performance parameters.

Keywords- Image Watermarking, Discrete Wavelet Transformation, Advanced Encryption Standards and Back Propagation Neural network.

I. INTRODUCTION

Image watermarking is the act of abstract a message correlated to a digital signal within the signal itself [1]. It is an idea closely related to steganography, in that they together hide the message inside a digital signal [2]. Watermarking helps to abstract a message regarded to the real idea of the digital signal, the digital signal in the steganography no relative to the message, and it is merely used as an original image to abstraction its existence. Digital watermarking defines the procedure of implanting some extra information into a digital broadcasting, deprived of compromising the media's significance [3]. This added data is labeled as watermark and also this watermark is secreted by means of an embedding algorithm in such particular manner in which it may possibly be unnoticeable to a human spectator, but then again easily recognized through a specialized recognition algorithm. To some extent, watermarking method should obligatory accomplish few of the vital watermarking properties as well as it ought to be precise to the particular application domain [4][5].

Different types of watermarking explained in below paragraphs:

A. Blind/Public watermarking: The original data is not needed during the detection process when detecting a mark, that watermark is measured to be blind/public. The solitary thing mandatory is the data utilized to create the watermark originally, comparable to a key which might've been utilized as a portion of the procedure to find out the actual watermark for a photograph [6].

B. Private/non-blind watermarking: The unique information as well as the private key is essential through the discovery practice, it's deliberated to remain a private or non-blind watermarking.

C. Asymmetric/public-key watermarking: In this, neither the unique material, nor a private key is compulsory for the period of the recognition procedure, it's considered to be present as an asymmetric/public-key watermarking [7]. Private Key is mostly used to construct the sign, but then again independently a public key is needed to validate the watermark (exactly like how a digital signature is checked in cryptography).

The work is scheduled as gives a types of the Text watermarking in section I and overview of text watermarking II; a study of the literature of these approaches and techniques for to reduce the time and increase with the image quality module in section III. It used for proposed algorithm or simulation is described in section V succeeded by the research technique. Here discussed the problem formulation in section IV, The evaluation of performance parameters and consequences followed by the conclusion and future scope in section VI.

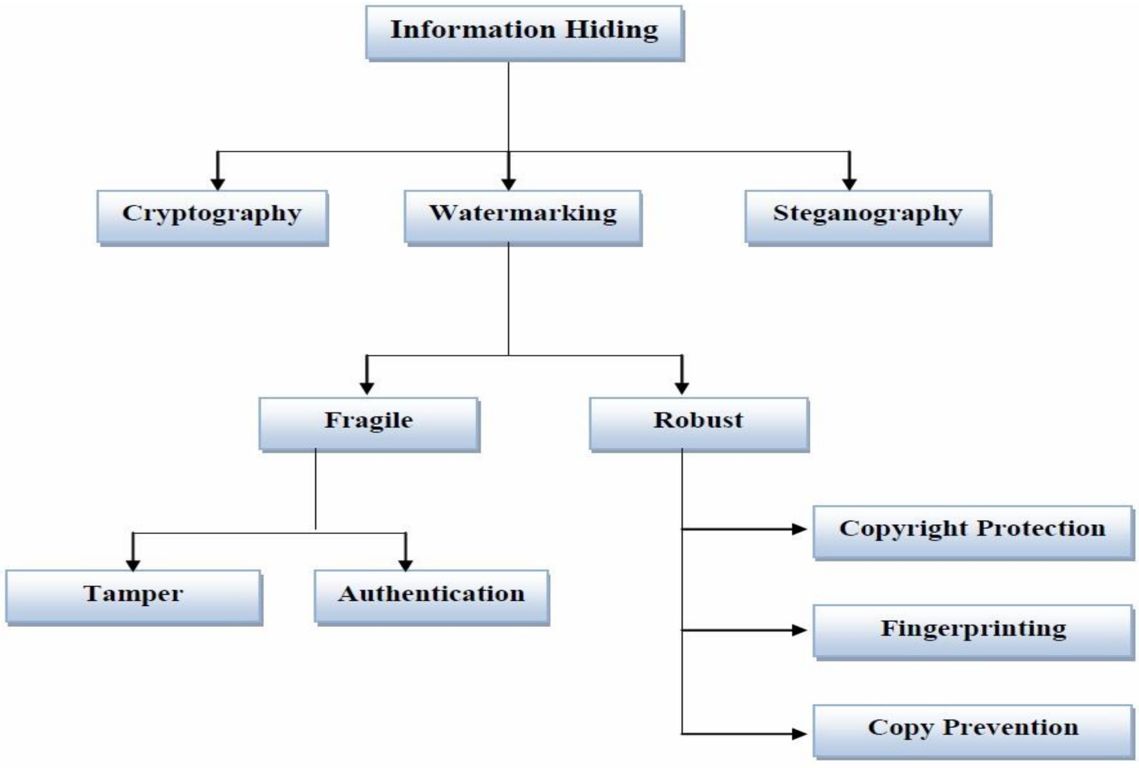

Fig 1: Types of Information

II. OVERVIEW OF IMAGE WATERMARKING

Watermarking a depiction is one of the numeral data that can be watermarked. A simple algorithm may flip the last bit of data representing each pixel in each photograph. Therefore, the picture will extreme likely not be obviously different as of the exclusive picture since altering any of blue, red, or green, smallest significant bit will not impact the depiction all that ample[8]. This is smearing a watermark in the direction of a spatial domain. There's another method of attractive a watermark by way of addition it to aoccurrence domain. For instance, a discrete may possibly create pictures which go by various alterations similar to Fast Fourier Transform in development on applying some waterline, and then make a transposed transformation to acquire the actual picture.

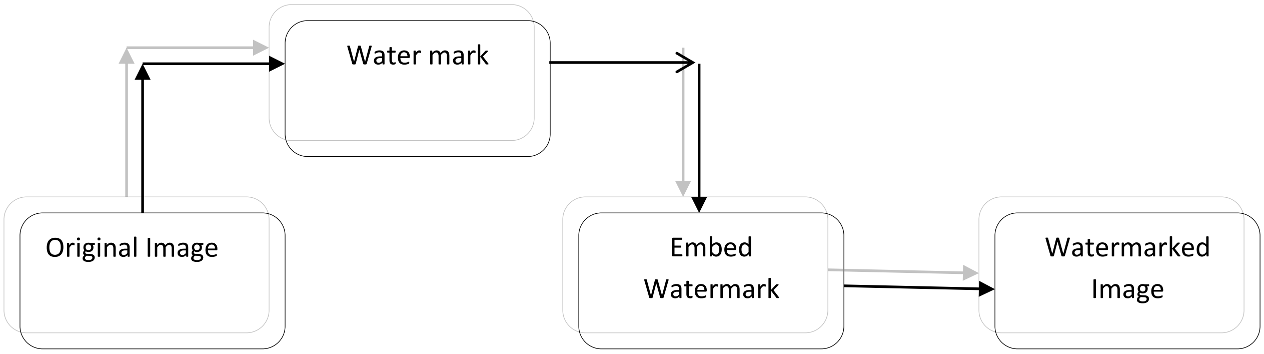

Fig 2: Image Watermarking Process

A. Features

An operational watermark ought to have numerous properties, showed further down, whose significance will differ reliant upon the application. There are numeral amount of researcher work's that have argued about numerous features of watermarks [9]. Approximately few of the features conversed are robustness, imperceptibility, security, un-detectability, and capacity. In practice, it is not probable to plan a watermarking scheme that outdoes at all of these. Each and every watermarking method creates tradeoffs amongst them, taking into consideration about the application domain. In the next subsections we explain each of the features stated above, as well as talk over in what way its significance as well as its explanation differs with application. The essential features of watermarking are given as follows:

- Robustness
- Security
- Imperceptibility
- Capacity
- Fragility

III. RELATED WORK

Qing-Cheng Li(et.al) [10] proposed as, a novel text watermarking method but for the Chinese text merely. In his or her method he's mentioned this some bitstream pattern of the manuscript on the basis of which the integration can be done .His method also describes the pictographic approach of the text and the visual potential of the person. This method will be despite the fact that comes with a usefulthinking but the difficult is as the Chinese language is so cultured, it fits there but not with each and every terminology. Algorithm may be intended particularlyfor Chinese characters and hence this algorithm cannot be used for global language.Zeneca JaliI (et.al),[11] presented a zero text watermarking arrangement in the worldwide conference of 2010. Giving to them, existing text watermarking procedures are not robust in contradiction of random insertion and deletion attacks on specific text document. By means of growing volume of attack, the existence of watermark in the text document turn out to be stimulating and hence they developed a novel text watermarking procedure that can be used for right guard of textual materials. They will when matched their results along with various other existing algorithms of the same difference and their results are found to be effective enough to get proceeded for modification.Makarand L. Mali (et.al),[12] presented a watermarking scheme on the basis of NEURAL networks. It was a fantastic idea to introduce Neural Networks into the difference associated with encryption. The Neural Network produces weight for each and every input provided to it rather than taking all as an input stream. The decoration changing of neural network is moderately similar to SVM as it also changes the entire input rendering its simplification and then precedes .Hence his method was quite actual and can be considered for future development process.NidhiDivecha(et.al) ,[13]has proposed, a watermarking arrangement based on the wavelet quantization method which is again an considerableenergy in this filed. DWT stands for Discrete Wavelet Conversion and it adapts the entire data scenario into waves. Previous the texts as wave area exclusive method in this type of enactment. The time and effort accomplished simply by Nidhi had only one negative aspect , she did not reference the type of wavelet transformation she is using as there are a lot of wavelet conversion like Dabuchi, Symlet and others and hence her technique can be tried with the above mentioned wavelet family members. FahimIrfanAlam(et.al)[14] introduced the concept of signature in his scheme of watermarking. The signature structure is diminutive bit alike to the private and public key concept in which the public key is visible to all but it requires a secluded key to change to unlocked. If this technique is experimented underneath invisible watermarking concept, it is fine but if it is used as a observable watermarking concept, the reason of hiding of data remains unharmed as the user would be able to recognize easily that some data is hidden behind the encrypted text.

IV. EXISTING PROBLEMS

Lots of paper Study, we found Digital watermarking is the process of introducing a digital signal or pattern into digital satisfied. The signal, known as a watermark, can be used to identify the possessor of the work, to authenticate the content, and to trace prohibited copies of the work. A watermark is a form, image or text that is captivated onto paper, which offers indication of its authenticity [15]. Digital watermarking is an allowance of this concept in the digital world. Methods that used to watermark a digital image least significant bit algorithm. The system implements visible watermarking. With development of digital systems, the presentation of picture, digital cameras as well as audio devices is also better. The satisfied of digital picture/audio/video can easily be modified so that it is very difficult to detect what changes has been taken place. In the circumstance of quite delicate legal papers and medical pictures, this becomes progressively significant to verify the authenticity of original content. For verification, a watermark is entrenched in original satisfied which is used to appraise the strength of such type of content. If the data is changed via any attacker unkindly, the watermark gets different and therefore the content will be considered non-genuine. So, the existing work will use wavelet transformation along with evolutionary algorithm in hybridization.

V. PROPOSED WORK

In this section we define the proposed work in image watermarking. We applied the DWT technique for found the wavelets. AES algorithm used for secures the message in the two processes (i) Encoder and (ii) Decoder. Now, classify the secure message using Multi-layer architecture (Back Propagation Neural Network).

In methodology we will follow these steps:

Step 1 : First, we should take the plain image.
Step 2 : Then we will call DWT for image sub-division. The discrete wavelet transform is a valued way calculated for indication examination as well aspicture treatment, primarily in multi-resolution account. It can powder indication into dissimilar mechanisms in the incidence compass.

One-dimensional (1-D DWT) crumbles a contribution into 2 modules (the regular constituent & the feature constituent).

2-D DWT crumbles a contribution picture into 4 sub-bands, 1 normal constituent (LL) & 3detail mechanisms (LH, HL, HH) as shown in Figure 3.

LL	HL
LH	HH

Fig 3: Discrete Wavelet Transformation

Step 3 : Then the DWT component will be taken for watermarking.

Step 4 : Get image that is to be watermarked of same size or large size.

Step 5 : Then AES algorithm will be used for security or image watermarking. Stop

Step 6 : Then after this procedure it would be watermarked.

Step 7 : Last one Classify the watermark images for training and testing.

Step 8 : In the end, we will evaluate the results based on BER, PSNR and MSE parameters.

Pseudo Code of the AES Encryption:

We proceeds to the subsequent steps to encode a 128-bit block:

- Develop the group of round keys from the cipher key.
- Initialize the state array using the block data (i.e. plaintext).
- Add the primary round key to the beginning state array.
- Execute9th rounds of state manipulation.
- Execute the 10th as well as the final round of state manipulation.
- Duplicate the finishing state array out as the encoded data (cipher text).

Pseudo Code of AES Decryption:

Decryption includes reversing completely all the steps taken in encryption using inverse functions.

- Execute the initial decryption round of state manipulation.
- Execute nine full decryption rounds of state manipulation.
- Perform final round of state manipulation.
- Copy the finishing state array out as decode (decrypted) data.

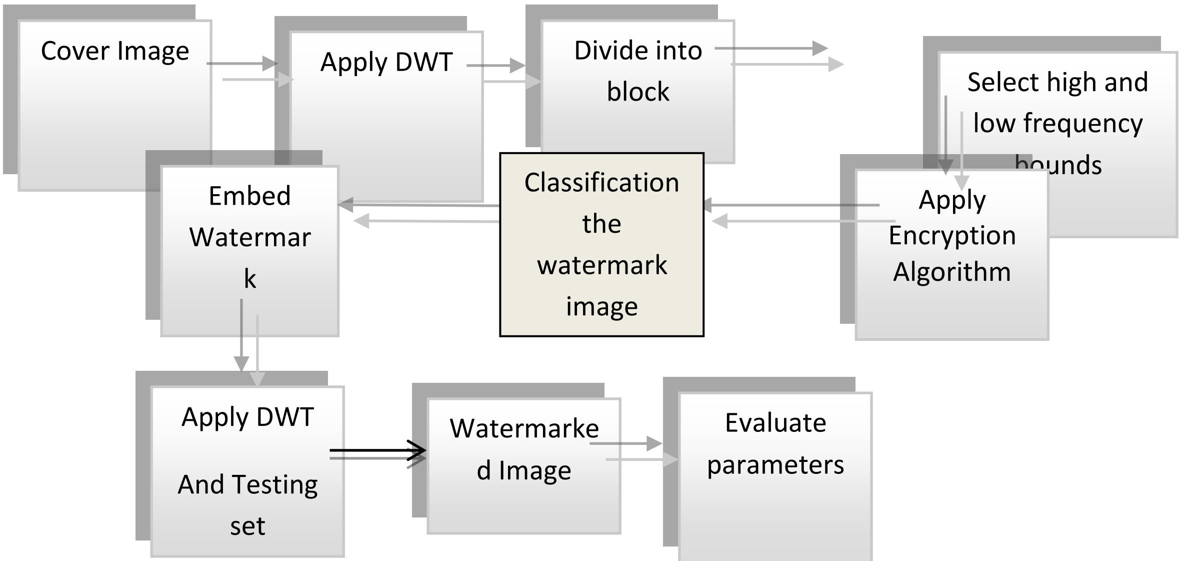
Cover Image
Apply DWT
Divide into block
Select high and low frequency bounds
Embed Watermar k
Classification the watermark image
Apply Encryption Algorithm
Apply DWT And Testing set
Watermarke d Image
Evaluate parameters

Fig 4: Proposed Flow Chart

VI. CONCLUSION

This paper defines that use of back propagation Neural Network algorithm that is applied to the lsbtechnique,with benefits of hiding the trained network weights with the real cover image. Watermarked image has a good robustness and the imperceptibility of the cover image is also highly preserved. For the extraction, only cover image is required and no external weights files need to be supplied with the watermarked image. Thus, this effort leads to a successful watermarking scheme. We have outlined an approach to embed a nearly invisible watermark into an image. Although it said to be nearly invisible, it is to find out the watermark visually, for a careful observer. On the other hand, the watermark is unique to individual image, and will be destroy completely in case of small modification, which is a property to against hacking. Result we shows in second paper.

VII. REFERENCES

[1]. ZuneraJalil and Anwar M. Mirza, “A Review of Digital Watermarking Techniques for Text Documents”, IEEE International Conference on Information and Multimedia Technology, pp. 230-234, 2009.

[2]. Yanqun Zhang, “Digital Watermarking Technology: A Review”, IEEE International Conference on Future Computer and Communication, 2009.

[3]. Robert, L., and T. Shanmugapriya, A Study on Digital Watermarking Techniques, International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.

[4]. B. Macq and O. Vybornova, “A method of text watermarking using presuppositions,” in Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, vol. 6505, San Jose, CA, January 2007.

[5]. O. Vybornova and B. Macq, “Natural language watermarking and robust hashing based on presuppositional analysis”, IEEE International Conference on Information Reuse and Integration (IRI), Las Vegas, Ireland, September 2007, pp. 177-182.

[6]. Cox and M. L. Miller, “A review of watermarking and the importance of perceptual modeling”, Proceedings of SPIE, Human Vision and Electronic Imaging II, vol. 3016, 1997, pp. 92–99.

[7]. J. Cox and J.-P. Linnartz, “Some general methods for tampering with watermarks”, IEEE Transactions on Selected Areas of Communications, vol. 16, no. 2, 1998, pp. 587–593.

[8]. F. A. P. Petitcolas, R. Anderson, and M. G. Kuhn, “Information hiding - A survey”, Proceedings of the IEEE, vol. 87, no. 7, 1999, pp.1062– 1077.

[9]. R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, “Perceptual watermarks for digital pictures and video”, Proceedings of the IEEE, vol. 87, no. 7, 1999, pp. 1108–1126.

[10]. “Qing-Cheng Li “Novel Text Watermarking Algorithm based on Chinese Characters Structure “,2008 International Symposium on Computer Science and Computational Technology

[11]. “ZuneraJaliI,Hamza Aziz Saad Bin Shahid\ Muhammad Arif “A Zero Text Watermarking Algorithm based on Non-Vowel ASCII Characters 978-1-4244-8035-71101$26.00 © 2010 IEEE

[12]. Makarand L. Mali “Implementation of Text 2013 International Conference on Communication Systems and Network Technologies Watermarking Technique Using Natural Language Watermarks.

[13]. “NidhiDivecha” Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color pictures 2013 International Conference on Intelligent Systems and Signal Processing (ISSP).

[14]. ” FahimIrfanAlam “An Investigation into picture Hiding Steganography with Digital Signature Framework 978-1-4799-0400-6/13/$31.00 ©2013 IEEE.

[15]. ManjitThapa,"Digital picture Watermarking Technique Based on Different Attacks”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011.