Comparative Analysis of Analytic Measures of Discrete Wavelet Transform Methodology in Gray-Scale and Color Images

S.Thilagamani, K.Prem Kumar

Abstract: ***The advent of modern technology makes the lives of the mankind easier and faster. But the fact is data emerged in the network field subjects to produce false record of data. Hence, the preservation mechanism of data is much needed in every region of the field. Image watermarking is the one of the vital key feature behind the security measure. This methodology helps in the enclosure of data over the other inorder to provide security. Thus, the secret data is hidden across the transmission from being attacked by the third party individual. The proposed work gives the safer means of data enclosing specially for providing secrecy towards the system.***

Keywords: Discrete Wavelet Transform; gray-scale image; Arnold transform; digital watermarking

I. INTRODUCTION

Digital watermarking the methodology of enclosing the data one over the other. This provides the security from the un-authorized person by eliminating the generation of false results, removal of data, providing unwanted information, replacing the original content etc. Generally, the watermarking technology is a two-step process. First, is the enclosure phase process and second is the extract phase process. The first phase of the process is the enclosure process that enclose the key image within the original host image. The next phase is the extraction that draw out the hidden key image from the input host image. The embedded and draw out key image is actually the watermark. The advancement in the computer technology gives many advantage like viewing the geographical news at your place, internet based communication, downloading some media such as pictures, music, movie, entertaining news etc. Apart from the advantages, it have the issues in terms of unauthorized user using illegal information across the web. The usage of internet provides complication in terms of infringement and copyright conflict. The information has to be secured by implementing some of the cryptographic measures. For the other various reasons, the encryption of data or information is needed to eliminate conflicts in copyright policies. To avoid this conflicting measures, watermarking technique is introduced [1].

Revised Manuscript Received on June 05, 2019

Dr.S.Thilagamani, Professor& Head, CSE, M.Kumarasamy college of Engineering, Thalavapalayam, Karur, India
Mr.K.Prem Kumar, Assistant Professor, CSE, M.Kumarasamy college of Engineering, Thalavapalayam, Karur, India.

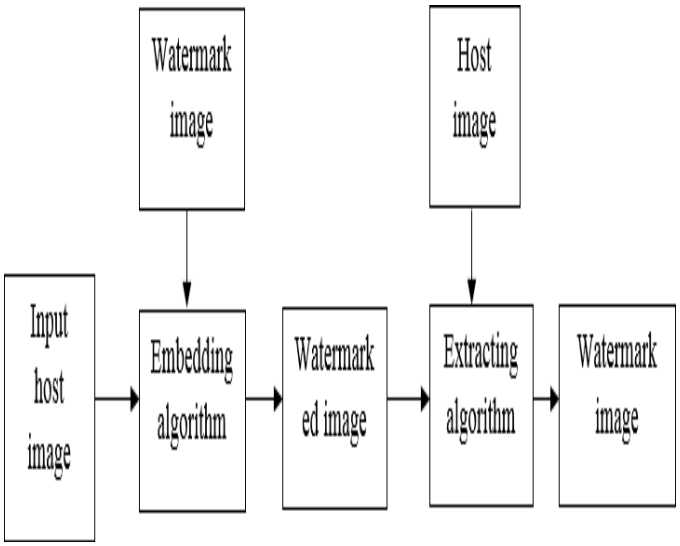

Fig. 1. Digital Watermarking

There are many techniques available so far that provides secrecy over the data or information. Apart from the various benefits available in the existing work, there are some complication too. This may reduce the robustness of the system. Inorder to make the system more robust and secure, a system must be proposed. The method is proposed that uses the gray- scale and color images as the input. Discrete Wavelet Transform (DWT) is applied to the input images as soon as the pre-processing techniques are applied. This splits the image into 4 bands based on the low and high contrast available on the region. The watermark is then added to the separated bands of the DWT outcome. To ensure the strength of the proposed work, some image processing attacks are implemented. By using the implemented attacks, some of the parametric calculation are computed. From the parametric computed value it is proved that the proposed work withholds strong encryption despite of the attack.

II. RELATED WORKS

[1] The emerging need is required for providing the secrecy over the important

data, as the development in the recent technology holds its positive point in one hand. On the other hand it leads to hazards in terms of piracy and copyright policies. To maintain the secrecy the watermarking technology is proposed. This technique is based on Fractal encrypting and Discrete Cosine Transform (DCT). To enhance the classic DCT technique, the proposed work fuses fractal encryption and DCT for double encoding. For first encryption, the fractal encryption is performed to the image taken as input. DCT method is used for the second encoding along with some parametric measure. The fractal encryption is induced to encrypt the confidential image with the personal data. Encrypting terminologies are incorporated for digital watermarking, which is applied to the input image. This helps to draw out the confidential data from the image. The parameters are calculated which shows that this system have higher result towards its performance when compared to classic technology.

[2] The introduction in the computer based technology have many serious defects despite of the available merits towards the system. This paper presents various watermarking techniques and the commonly available attacks in the watermarking system. The commonly available watermarking techniques include spatial and transformation technology.

- Spatial watermarking: This method of technique embeds the watermark in few pixels of the input image. From the corresponding pixels the embedded data is extracted. This methodology is ease in usage and takes lower time for computation.
- Transformation based watermarking: It is advanced to the spatial watermarking technique, as it uses some of the pre transformation followed by which the watermark is embedded to the input image. The most commonly available transformation watermarking techniques are Discrete Cosine Transform, Discrete Wavelet Transform and Discrete Fourier Transform.

Fig. 2. Gray-scale image (a) Input host image (b) Watermark image

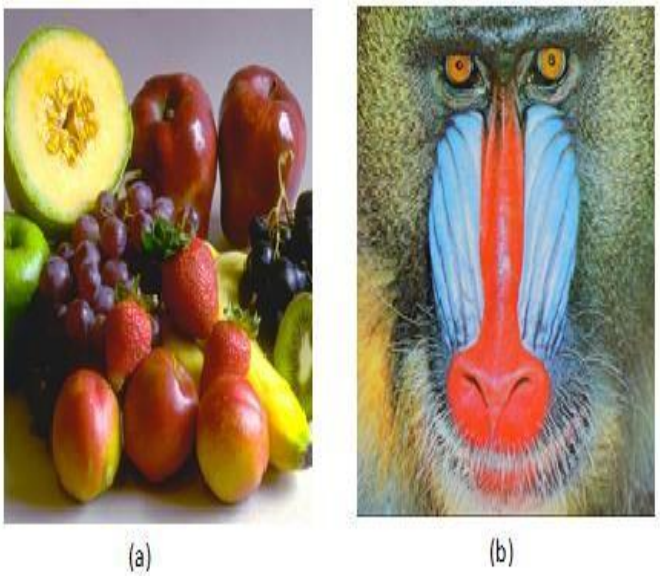

Fig. 3 Color image. (a) Input host image (b) Watermark image

The watermarking attacks available are as follows active, passive, geometric, degradation of image, removal, filtering etc. The attacks are located in the watermark when it is being transferred.

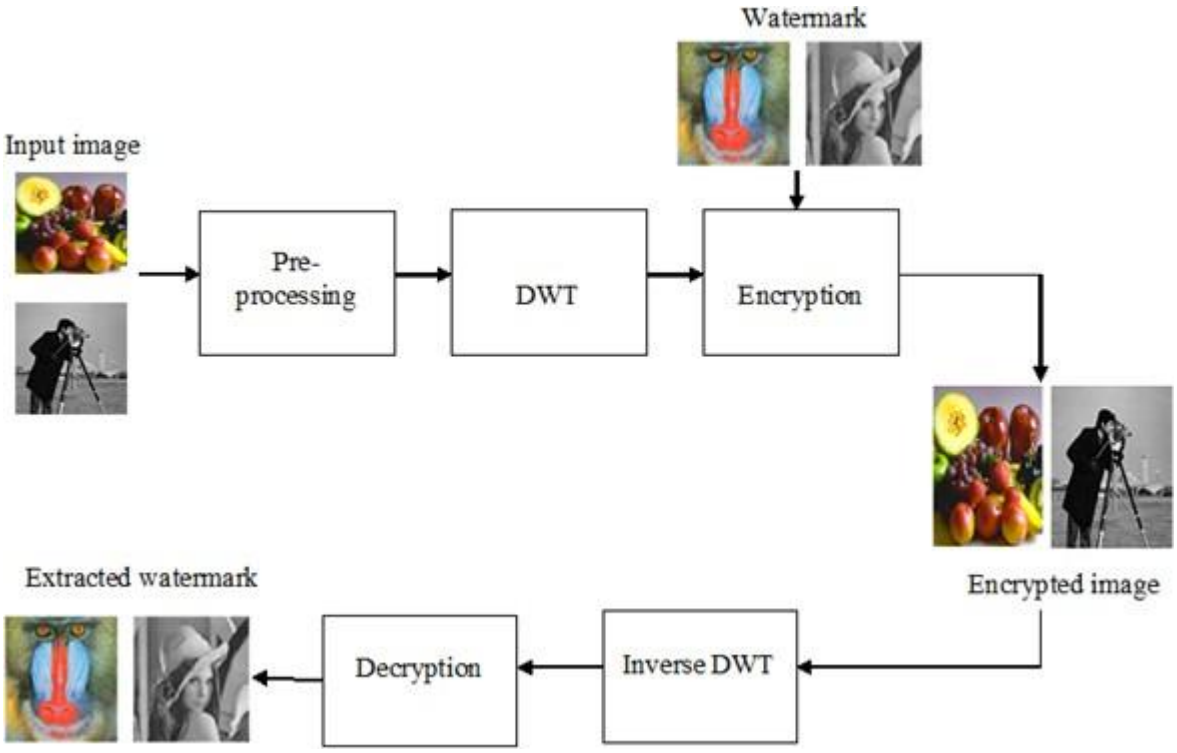

Fig. 4 Proposed architecture

[3] The digital watermarking techniques aims in adding the confidential data in the input image without damaging the quality of the image. This work is based on Discrete Wavelet Transform (DWT) accompanied by Singular Value Decomposition (SVD). It uses the images separated into blocks by utilising the entropy strategy. The image block having low entropy value is considered for the watermark embedding. Once the significant region is selected for embedding, the SVD is appliedto the lower bands of U matrix of the DWT result. The experimental observation shows that the proposed work have higher robustness and undetectable secret value. The inverse of DWT and SVD gives the extraction of the watermark for the image taken as input for the performance.

[4] The technique is proposed that combines multi hybrid watermarking method along with the combination of Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD). This work applies the transformation together despite of the individual implementation of the technique. The collective watermarks are encoded in the single medical picture. This produces the higher robustness and undetectable nature enhancing more security and safety. The watermark is embedded by combination of all the three decomposition measure.

based watermarking scheme is increasing towards its performance due to the origin of wavelets. The important data to be made secret is hidden in the original information to provide originality of the input data.

III. METHODOLOGY

The watermark is hidden in the input cover image and by the inverse of DCT and SVD methodology. The extraction is carried out by using the proper algorithm for draw out of watermark. Whereas in the next level, the text is encoded as the watermark. The outcome of the system is analysed by gain factor, volume and input medical cover image taken in various measures. By analysing the measure calculated it is found that the proposed work holds good against the attack performed.

[5] The security towards the multimedia components like image, video, text, audio files suffers dangerous hazards. They are being edited and malfunctioned by various technology. Providing the authentication and originality has become a serious problem. The editing mechanism is performed in the information such that it looks as if the original information. As a result it is found that the differentiation between the original and morphed data could not be detected. Nowadays the various problems are created for the multimedia data that creates the issue in the originality, copyright policies and unwanted editing of information without the author concern. For this the digital watermarking is used to prevent the important data in the digital form. Various digital watermarking methods are used for preventing the digital data that are based on the dimensional and density domain. The density

The proposed methodology includes the following components as pre-processing of input host images, performing DWT, embedding watermark, performing inverse of DWT, extracting the watermark, imposing attacks and calculating the

performance metrics. The components along with its description are given as follows:

A. Image Preprocessing

The input host image as well as the watermark is made to be processed before performing the required methods for watermarking. This will help in rectifying the noise in case of its presence.

B. Discrete Wavelet Transform

The pre-processed image is subjected to perform DWT to divide the host image into four region namely LL, LH, HL, HH. It is divided based on the contrast of the image region. The region having visible information is made to undergo encoding of watermark image. The 8x8 square wavelet is generated as a result of DWT.

C. Encrypting Watermark into host image

As an initial step, the RGB based color image is converted to gray scale image. The watermark having the scaled factor of constant x is added to the cover image. The watermark to be embedded is also made to undergo the DWT process. The watermark is embedded in the corresponding DWT band potion of the original cover image.

D. Attacks

The image processing attacks are induced in the process of proposed work to check the integrity and robustness of the work proposed. About five attacks are introduced in the proposed work namely, Gaussian noise attack, histogram, geometric attack, salt and pepper noise and cropping. The attacks are made to impose on the image embedded with the watermark i.e. the watermarked image. The results of various attacks are detailed in the chart as shown in the figure fig.5.

E. Extracting the watermark

The embedded watermark is draw out from the original cover image by subtracting the added constant value to the cover image. This is performed by v=v-x, where x is the constant added for the encoding of watermark to the image.

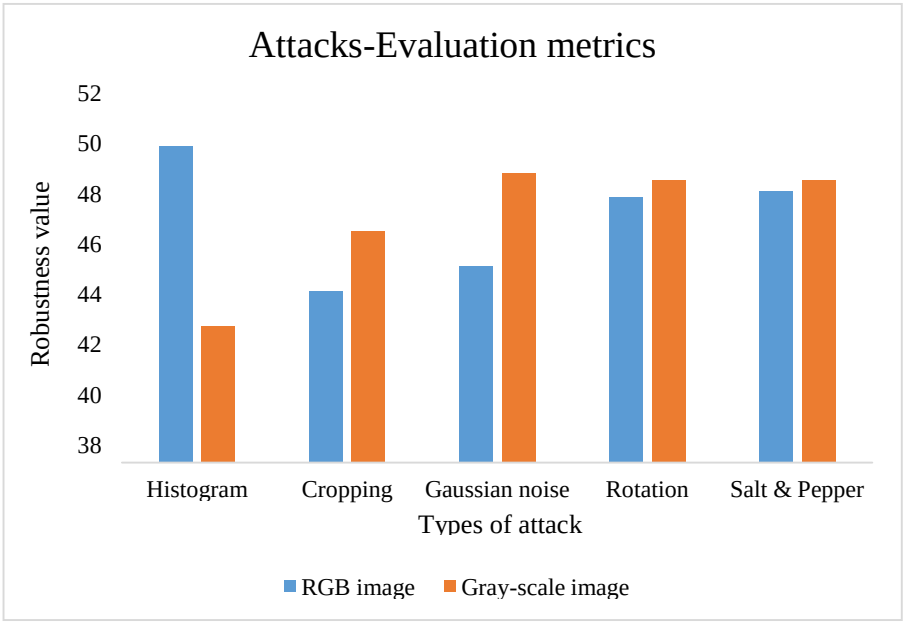

Fig. 5.Evaluation metric

IV. CONCLUSION

It is found that the watermarking plays an important role in terms of providing the secrecy over the transfer of data. This proposed work uses the DWT methodology for embedding the watermark to the original cover image. From the evaluation measures computed it is found that the both grayscale and color image more or less have the nearby values as per the computed results. It shows that DWT based encryption system provides approximately equal robustness and originality in the information.

REFERENCES

1. Shuai Liu, Zheng Pan, Houbing Song, "Digital image watermarking method based on DCT and fractal encoding", Advances in Big Data Methods for Image Processing , doi: 10.1049/iet-ipr.2016.0862, www.ietdl.org
2. Sonam Tyagi, Harsh Vikram Singh, et.al, "Digital Watermarking Techniques for Security Applications", International Conference on Emerging Trends in Electrical, Electronics and Sustainable Energy Systems (ICETEESES– 16), 978-1-5090-2118-5/16/$31.00 ©2016 IEEE
3. Nasrin M. Makbol, Bee Ee Khoo, et.al, "Block-based discrete wavelet transformsingular value decomposition image watermarking scheme using human visual system characteristics", IET Image Processing, doi: 10.1049/iet- ipr.2014.0965 www.ietdl.org
4. Amit Kumar Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images", Multimed Tools Application, DOI 10.1007/s11042-016-3514-z,2016.
5. Anuja Dixit, Rahul Dixit "A Review on Digital Image Watermarking Techniques", I.J. Image, Graphics and Signal Processing, 2017, 4, 56-66 Published Online April 2017 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijigsp.2017.04.07.

AUTHORS PROFILE

Dr. S. Thilagamani received the B.E. degree in Computer Science and Engineering from Periyar University, Salem, Tamil Nadu, India in 2002 and the M.E. degree in Computer Science and Engineering from Anna university, chennai, Tamil Nadu, India in 2007 and secured university second rank. She received her Ph.D. degree from Anna University, Coimbatore in June 2014. She has teaching experience of about 14 years. Presently working as Professor & Head in the Department of Computer Science and Engineering at M.Kumarasamy College of Engineering, Karur. She has published 14 papers in the reputed international journals. She has received award for best administration.. She is an active member of CSI and coordinator of CSI student branch. Her area of interest is Data Mining.

K.Prem Kumar received B.Tech degree in Information Technology from Anna University, Chennai in the year 2010. He received M.E degree in Computer Science and Engineering in the year 2015 from Anna University, Chennai. Currently He is working as Assistant Professor in Department of Computer science and Engineering at M.Kumarasamy college of Engineering, Karur. His research area is Data security.