ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 5, Issue 3 (July - Sept. 2017)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2017)

Reliable Fuzzy Embedding Technique for RGB Image to Secure the Image Transmission

[I]Dimpy Ahuja, [II]Deepika Arora
[I]M.Tech Student, Dept. of Computer Science, RPIIT/Kurukshetra University, Haryana, India
[II]Assistant Professor, Dept. of Computer Science, RPIIT/Kurukshetra University, Haryana, India

Abstract
Watermarking is the technique of embedded any information into another image.A watermark may be in many different forms which may act as host or the guest depending on what is being embedded into which. It acts as a digital signature, giving the image a sense of ownership or authenticity. Digital watermarking technique is very impressive for image authentication or protection for attacks. The proposed work is based on DCT technique which explains how a data can be embedded securely in the image. The proposed work is inspired by the genetic approach, in our work we have implemented the training of the images using GA or DCT which shows its histogram form and optimizes the images for further processing. With an embedded image containing additional data, onlythe authentic person can extract the information from the embedded one. He can extract the additional data though receiver does not know the image content. If receiver has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. The proposed work is supported on the GUI model which gives a practical implementation of the work. The work is implemented on the MATLAB software and different aspects have been considered.

Keywords
Digital Watermark, Steganography, Authentication, Frequency Domain, Spatial Domain, Least Significant Bit, GUI.

I. Introduction

The sudden increase in watermarking interest is most likely due to the increase in concern over copyright protection of content. The Internet had become user friendly with the introduction of Marc Andreessen's Mosaic web browser in November 1993, and it quickly became clear that people wanted to download pictures, music, and videos. The Internet is an excellent distribution system for digital media because it is inexpensive, eliminates warehousing and stock, and delivery is almost instantaneous. However, content owners (especially large Hollywood studios and music labels) also see a high risk of piracy. This risk of piracy is exacerbated by the proliferation of high-capacity digital recording devices. When the only way the average customer could record a song or a movie was on analog tape, pirated copies were usually of a lower quality than the originals, and the quality of second-generation pirated Copies (i.e., copies of a copy) was generally very poor. However, with digital recording devices songs and movies can berecorded with little, if any, degradation in quality.

A. Digital Watermarking

Digital watermarking is a technology for embedding various types of information in digital content. In general, information for protecting copyrights and proving the validity of data is embedded as a watermark.

1. Types of Watermarking

Public/blind watermarking

When the original data is not needed during the detection process when detecting a mark, that watermark is considered to be blind/ public. The solitary thing mandatory is the data utilized to create the watermark initially, similar to a key which might've been utilized as a portion of the procedure to find out the actual watermark for a photograph.

Private/non-blind watermarking

The unique information as well as the private key are essential throughout the discovery procedure, it's deliberated to remain a private or non-blind watermarking.

Asymmetric/public-key watermarking

In this, neither the unique information, nor a private key is compulsory for the period of the recognition procedure, it's deliberated to be presents an asymmetric/public-key watermarking. Private Keys mostly used to construct the sign, but then again individually a public key is needed to validate the watermark (exactly like how a digital signature is checked in cryptography).

B. Image Watermarking

Watermarking a picture is one of the digital 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 utmost likely not be conspicuously dissimilar as of the unique picture since altering any of blue's, red, or green, smallest significant bit will not impact the picture all that ample. This is applying a watermark in the direction of a spatial domain [3, 4].

C. Watermarking Features

The essential features of watermarking are given as follows:
ROBUSTNESS 2. SECURITY 3. IMPERCEPTIBILTY
4. CAPACITY
5. FRAGILITY

II. Literature Survey

V.Santhiet.al Due to the advancement in Computer technology and readily accessible tools, it is quitesimple for the unfamiliarusers on the way to produce illegal copies of multimedia data which are floating across the Web. With the purpose of protecting those audio-visual aidinformation on the Internet many techniques are available including various steganography methods, encryption methods, information covering methods, andwatermarking methods. Digital watermarking is a methodthat a piece of digital information is embedded into an picture and extracted later for ownership authentication. Top-secret digital information could possibly be implanted moreover in spatial domain or in frequency domain of the cover information. In this paper, a different singular

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

value decomposition (SVD) and discrete wavelet transformation (DWT) based technique is proposed for hiding watermark in full frequency band of color pictures (DSFW). The quality of the watermarked picture and extracted watermark is measured using peak signal to noise ratio (PSNR) and normalized correlation (NC) correspondingly. It is witnessed that the superiority of the watermarked picture is maintained with the worth of 36dB. Robustness of proposed algorithm is verified for various attacks including salt and pepper noise and Gaussian noise, JPEG compression settingalong with cropping.

Prabhjot Kaur Cheema et.al, In the proposed technique components of English terminology including noun, pronoun, model verbs along with conjunctions associated with user's choice along with author id are used to create watermark of user's choice. Moreover, encryption techniques AES algorithm is applied to encrypt watermark and to enhance its security level to protect it from tampering attacks and to prove the most robust algorithm.

BidyutJyotiSaha et.al, In his work, a new spread-spectrum-like individually distinct cosine transform domain (DCT domain) watermarking technique for copyright protection of still digital pictures are investigated. The DCT is executed in blocks of 8 × 8 pixels as in the JPEG procedure. The watermark can encrypt data on the way to track illegitimate misuses. For flexibility commitments, the unique picture is not necessary during the ownership verification procedure, so it need to be demonstrated by noise. Double tests are involved in the proprietorship verification stage: watermark deciphering, that the message carried with the watermark will be removed, along with the watermark discovery that chooses no matter if a given picture contains a watermark generated with a definite key.

III. Problem Formulation

Watermark robustness is one of the major characteristics that influence the performance and applications of digital image watermarks. Robustness in this context means the ability of a watermark to resist common image processing. Watermarks can be categorized into three major groups based on their robustness: robust, fragile, and semi-fragile watermarks. Robust watermarks should be detected successfully in images that have been through manipulative distortions. Adversely, fragile watermarks are very sensitive and easily destroyed by image modifications. In the middle of both extreme ends are the semi-fragile watermarks. They can resist legitimate changes while being sensitive to severe tampering. Copyright protection concerns the positive identification of content ownership in order to protect the rights of the owner.

1. General Algorithm for watermarking

Step 1- Check the length of the watermark image to know how many copies will be embedded in the first LSB and if it will embed in the second LSB.
Step 2- Embedding the length of the watermark image in the first LSB.
Step 3- Convert the watermark image to bits.
Step 4- Inverse the watermark bit.
Step 5- Check the coordinate of X, if it is odd, the algorithm will add 1 to X, and if it is even, the algorithm will subtract 1 from X.
Step 6- Embed the watermark bit in the first LSB.
Step 7- Go to 4 until finishing the entire watermark.

IV. ProposedAlgorithm for Watermarking

First, we should take the plain image.

```
main_image=main_image;
```

Then we will call DCT for image sub-division.

```
max_l=max(lower);
min_l=min(lower);
max_u=max(upper);
min_u=min(upper);
```

Then the DCT component will be taken for watermarking.
ZMs of watermarked image are computed and stored in some register file to estimate rotation angle from rotated watermarked image.

```
current=dwt_upper{i};
training_set_upper(i,1:129)=current(1:129,1);
training_set_dct=dctimg{i};
training_set_ZMA=ZMA{i};
training_set_ZMO=ZMO{i};
```

To extract the watermark at detector end, the transformed (i.e. rotated) watermarked image is loaded that is to be watermarked of same size or large size.
Then GA algorithm will be used for image watermarking.

```
bitcount=1;
for j=1:100
Fs=bit_value(i,j);
   Ft=mean(bit_value(i,:));
FitnessFunction = @(e)fitness_fn(e,Fs,Ft);     %calling fitness function
numberOfVariables = 1;
    [xfval] = ga(FitnessFunction,numberOfVariables,[],[],[],[],[],[],[],options);
reduced_index=round(x);
ifreduced_index==1
GareducedFeaturesindex(i,bitcount)=1;

bitcount=bitcount+1;
set(handles.text2,'String',strcat('I:',num2str(i),'/3C:',num2str(j),'/100'));
end
```

Then after this procedure it would be watermarked.
In the end, we will evaluate the results based on PSNR, Time and MSE parameters.

```
global image myimageimage_new
tic;
I1=sum(sum(sum(image_new)));
I0=sum(sum(sum(myimage)));
myerror=I1-I0;
ifmyerror<0
myerror=-error;
end
mse=sqrt(myerror^2/(numel(image_new)));
psnr=10*log10(256^2/mse);
mytime=toc;
```

V. Results and Analysis

5.1 Below figure shows the main GUI of the proposed work containing various panels like Training panel and testing panel.

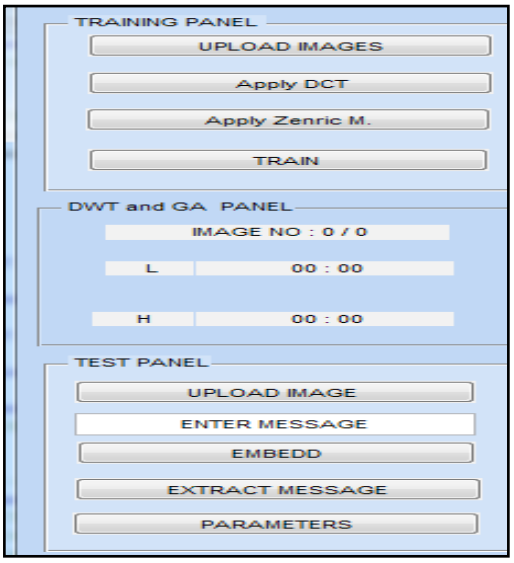

Fig 5.1

Now click on the upload icon and select the images for the training purpose. The screen shot showing the various images is shown below.

Fig. 5.2

The proposed work automatically trains all the images after selecting the one. The one of the several training images is shown below.

Fig 5.3

As the training is being done of the images the histogram plot based on DCT is plotted simultaneously on the right of the window as shown below in fig 5.4. The proposed work also shows the results of images based on DWT based on Lower and Upper bound as shown in fig 5.4-fig5.5

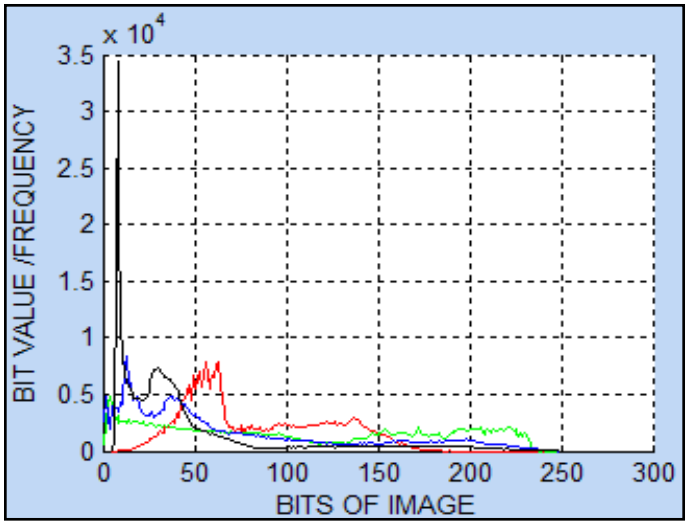

Fig. 5.4

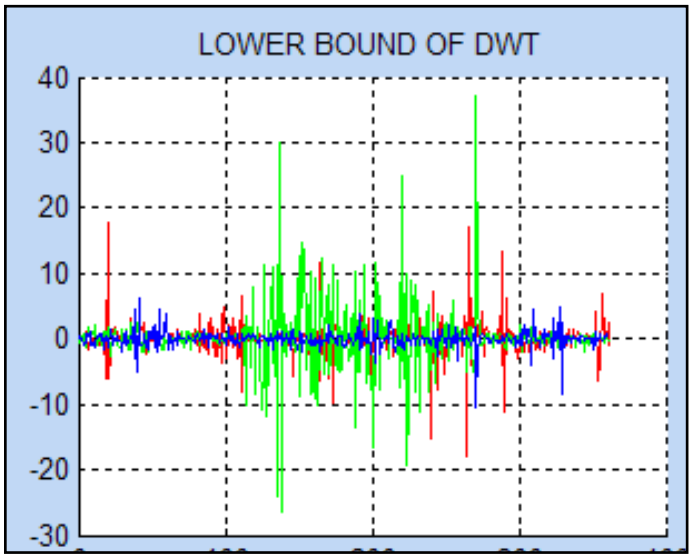

Fig. 5.5

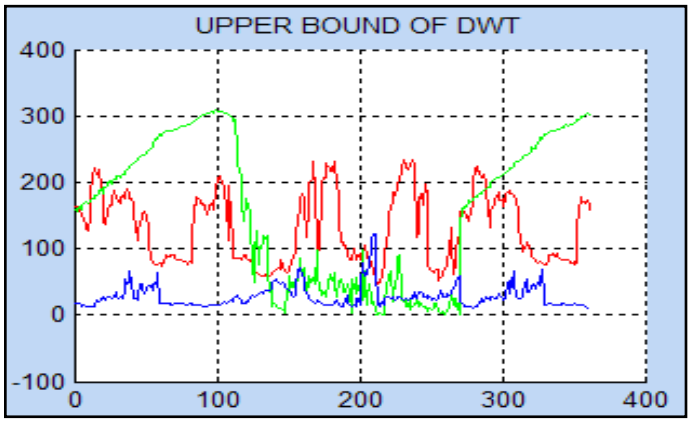

Fig. 5.6

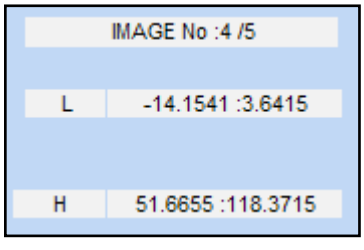

Fig. 5.7: Numerical analysis

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

After all this process, click on the icon **Apply DCT** and thefollowing result is obtained as shown in fig5.9

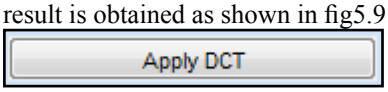

Fig. 5.8

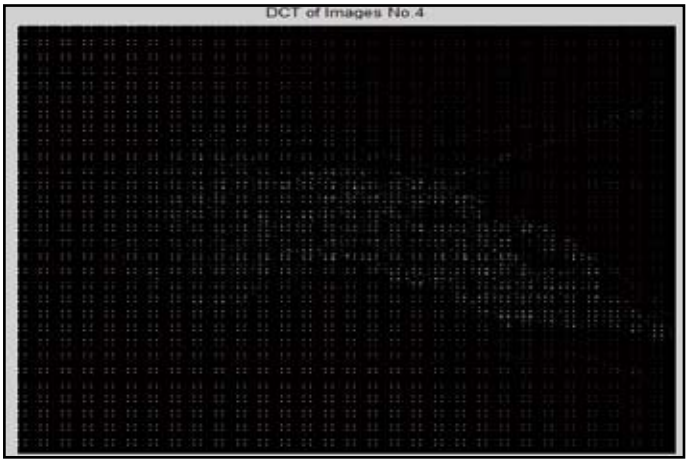

Fig. 5.9

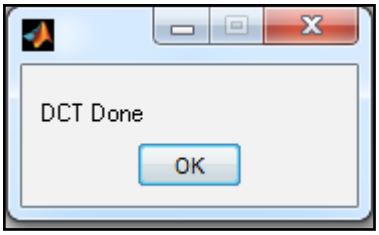

Fig. 5.10

Now click on the Train icon as shown to optimize the images using Genetic method.

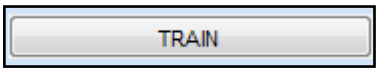

Fig. 5.11

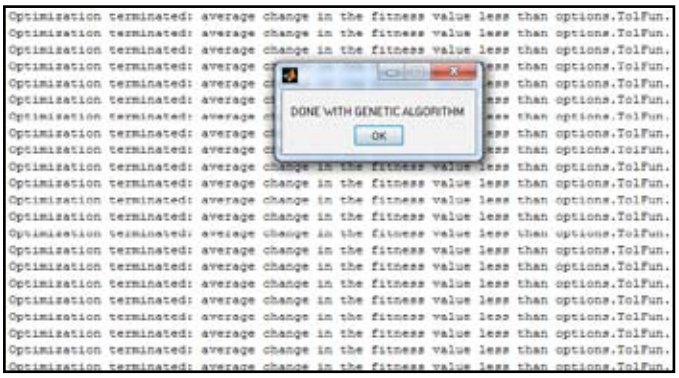

Fig. 5.12

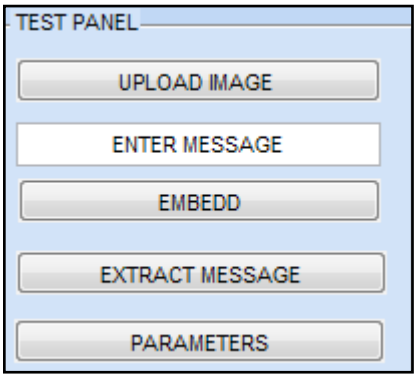

Fig. 5.13

Fig. 5.14: Cover image

Enter the message to be embedded with the cover image in the box below. Here for example we have write ENTERMESSAGE which is of 13 character.

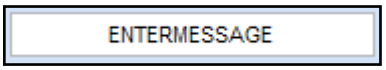

Fig. 5.15

On the basis of message we used the message will be encoded in the bits form as shown below in fig 5.16.

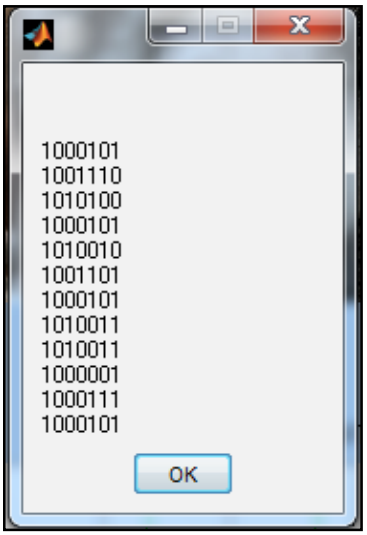

Fig. 5.16

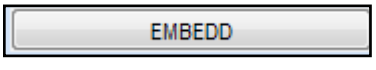

Fig. 5.17

After pressing the embedded button the stegno image will be created as shown below.

Fig. 5.18

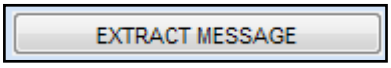

Fig. 5.19

After click on the extract message box the embedded message will be extracted from the image.

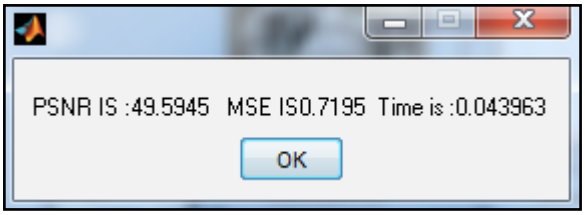

Fig. 5.20

Above figure shows the value of PSNR, Time and MSE for proposed method having values PSNR= 49.59, time= .719 and MSE = .07195.

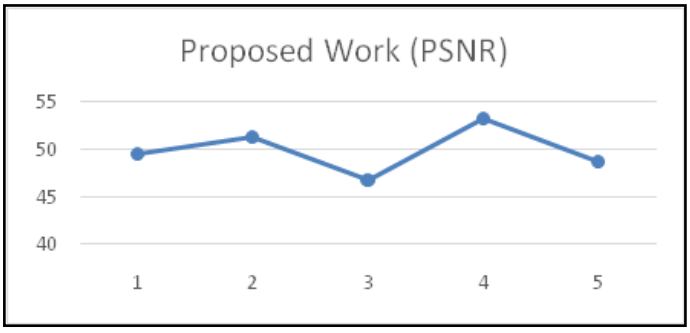

Fig. 5.21

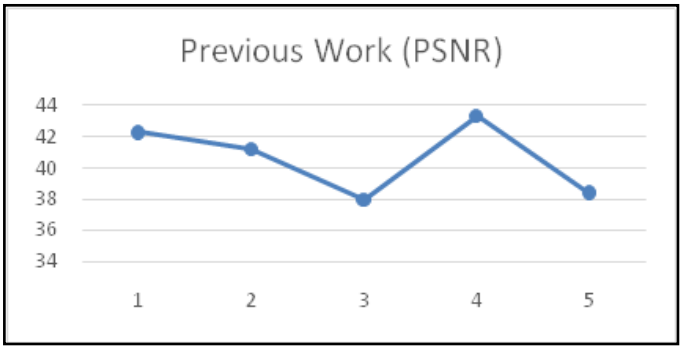

Fig. 5.22

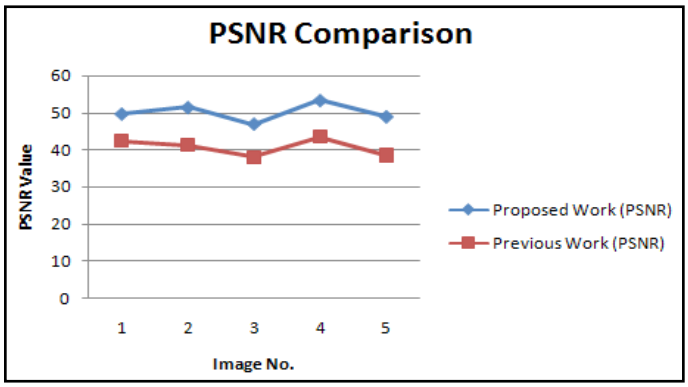

Fig. 5.23

Conclusion and Future Scope

Watermarking is a very active research field with a lot of applications. Although it is a relatively new field, it has produced important algorithms for hiding messages into digital signals. These can be described by many different methods. In this work, we proposed a method for watermarking based on the secure embedding of blind and multi-bit watermarks based on 2-level DCT using Genetic Algorithm (GA). When we use 2-level DCT then PSNR is increased and MSE decreases as compared to single-level DWT. Watermarking technique is applied withDCT using GA. Wavelet Transforms plays an important role in communication security where time, memory usages and battery power are the major issue of concern.The future work can be further extended with different formats of image using different encryption keys. By first encoding the message with a pseudorandom sequence, we could increase the security of the message. If the encoder uses the pseudorandom sequence with the message as a seed to select which segments are encoded, the decoder can only find what the original message was if he also has the sequence length.

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] *I. 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] *I. J. Cox and J.-P. Linnartz, "Some general methods for tampering with watermarks", IEEE Transactions on*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

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] F. Hartung and M. Kutter, "Multimedia watermarking techniques", Proceedings of the IEEE, vol. 87, no. 7, 1999, pp.1079–1107.

[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 TechnologiesWatermarking 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

[16] FRANK HARTUNG," Multimedia Watermarking Techniques", 0018–9219/99$10.00 ã 1999 IEEE PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999

[17] Mauro Barni," A DCT-domain system for robust picture watermarking", Signal Processing 66 (1998) 357Ð372

[18] Juan R. Hernández," DCT-Domain Watermarking Techniques for Still pictures: Detector Performance Analysis and a New Structure". IEEE TRANSACTIONS ON PICTURE PROCESSING, VOL. 9, NO. 1, JANUARY 2000

[19] V.Santhi," DWT-SVD Combined Full Band Robust Watermarking Technique for Color pictures in YUV Color Space", International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009 1793-8201.

[20] Prabhjot Kaur Cheema1, Kamaljit Kaur2, "Comparison of Text Watermarking Approaches with the Proposed Approach Based on Encryption Techniques used for Creating Watermarks"

[21] BidyutJyotiSaha, Kunal Kumar Kabi, Arun and Chittaranjan Pradhan, "A Robust Digital Watermarking algorithm using DES and ECC in DCT Domain for Color pictures" 2014 International Conference on Circuit, Power and Computing Technologies [ICCPCT]