International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-5 Issue-4, September 2015

Watermarking using Blind Embedding and Linear Correlation Detection

Md Khalid, Tazeem A Khan, A Shahid Khan

Abstract— Watermarking technology serves a vital role in information security. It focuses on embedding message (audio, image etc.) inside a digital object such that the embedded message is separate bound to the object. In this paper, I represent Blind Embedding and Linear Correlation Detection based algorithm for watermarking in digital images. I have used MATLAB for my proposed technique because it is a high level technical computing language for algorithm development, data visualization and numerical computations.

Index Terms—Watermarking, Blind Embedding and Linear Cor Relation Detection

I. INTRODUCTION

The accession of the internet and the easy use of computers and printers make digital data reception and transmission very easy. The digital data accessible through internet gives opportunities to any one for piracy of copyrighted data or message without permission of the message owner. Thus to avoid unauthorized use of message or data Digital Watermarking is used by which encryption and decryption of a message in digital format is done easily so that the message is used by authorized users only. It is also a process of information hiding. The watermarking process is applied to waveform type of information source, which allows any particular to add hidden copyright message or any verification message to digital image, audio and video etc. The main characterizations of a digital watermarking are as follow:

- Robustness
- Imperceptibility
- Capacity

The importance of each depends on the application how it is used. In the field of communication and information technology sector there is connection between the communication and computation which offers many chance for distribution and processing of important digital messages like text, images, audio tracks and movies. Thus, boom in technology makes easy for copying the data and use of pirated materials across the network. To get rid of this piracy, encryption and copyright principles is used so that only authorized users can use the data. Watermarking is the process by which we can easily encrypt and decrypt a data in digital format, then it can be used by only authorized users and unauthorized users will not be able to decrypt the data.

Manuscript published on 30 September 2015.
***Correspondence Author(s)**
Md. Khalid, Department of Electrical Communication Engineering, AFSET, MDU University, Dhauj, Faridabad, Haryana, India.
Tazeem A Khan, Department of Electrical Communication Engineering, AFSET, Al Falah University, Faridabd, Haryana, India.
Shahid A Khan, Department of Electrical Communication Engineering, AFSET, Al Falah University, Faridabd, Haryana, India.

II. WATERMARKING

A. *Properties of watermarking*

Robustness: It is the most desirable property of watermarking algorithm for copy protection. It depends on message capacity of watermarking, the watermark visibility and threshold value. It also varies by the selection of images in size, color depth and content. Effectiveness: It is the very important property of the watermarking. It is based on the probability of the message present in a watermarked image detected correctly. Ideally, we need this probability to be 1.
Image Fidelity: In watermarking, the original image is varied in adding a message to it, certainly the image quality gets affected. This degradation in image quality should be minimum so no change in the image fidelity can be seen.
Transparency: The encrypted watermarked pattern does not visually end the original image fidelity and needs to be perceptually invisible.
Payload Size: In watermarking, every watermarked work has to carry message. Therefore the size of the message is important as some system require only one bit to be embedded and some system require big payload to be embedded.
False Positive Rate: This is the counting of digital works that are recognized to have a watermark embedded when in fact it has no watermark embedded. This property should be low for watermarking system.
Security: Watermarked information must be secret and undetectable by any unauthorized user. This is security and it is achieved by cryptographic keys.

B. *Watermarking without Side Information:*

This is a communication based watermarking model in which image is imagined as another form of channel noise that distorts the message during its transmission. The terminology side information is verified as assisting signal apart from input signal which can be used for better encryption and decryption. In watermarking without side information this assisting or auxiliary signal is not available, the encryption and decryption is done by input signal only and by choosing any random variable of same dimension as the input signal have. The architecture of watermarking without side information is shown below:-

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

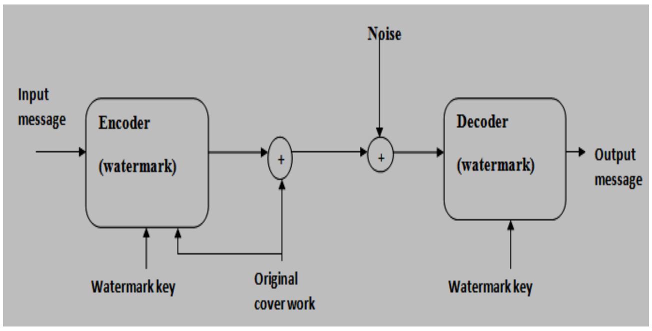

Fig.1 block diagram for watermarking without side information

There is a watermark embedder encoder which encodes the input message using a key. This embedded message is added to the original message or image and transmitted over the communication channel where some noise is added to it. The watermark detector at the receiving end receives the noisy watermarked image or message and it decodes the original message or image using key.

III. Blind Embedding and Linear Correlation Detection

This communication based watermarking system is a blind embedding system, which do not change the original image parameters to embed a message into an image. In this system detection is done by linear correlation detection. This system embeds only one bit(a 0 or 1) inside the cover image. Message or image pattern analyzing depends on what we are embedding. Embedding 0 results in taking negative to obtain the image or message pattern and if embedding is 1 then pattern will remain same.

This blind linear correlation technique embeds a pseudo random noise pattern with original image which has same size and dimension as original image have. The algorithm for encoder or watermark embedder and detector or watermark decoder is as follow:-

A. Embedder:

1. We chose a random reference pattern which is an array with the same dimension as of original image. The elements of this are drawn from a random Gaussian distribution having interval [-1,1]. To initialize the pseudo random number generator watermarking key is used that makes the random reference pattern.
2. Image pattern is calculated depending on embedding a 1 or a 0. If a 1 is taken then we leave the random reference pattern as it is. If we take a 0 , we take negative of the pattern to get the image pattern.
3. The message pattern is scaled by a constant α to control the strength of embedding. If the value of α is high we need more robust embedding otherwise we lose the image quality. The value used in the experiment is α= 1.
4. We add this scaled image pattern to the original image pattern to get watermarked image.

Detector:

1. The linear correlation between the watermarked image generated by embedder and the initial reference pattern that is generated using the initial seed which is the watermarking key is calculated.
2. From the result of correlation the watermark image is decided whether it is above the linear correlation threshold value or below it. If the value is above then the message was a 1 and if the value is negative then message was a 0. If the message is between the positive and negative threshold then no message was embedded.

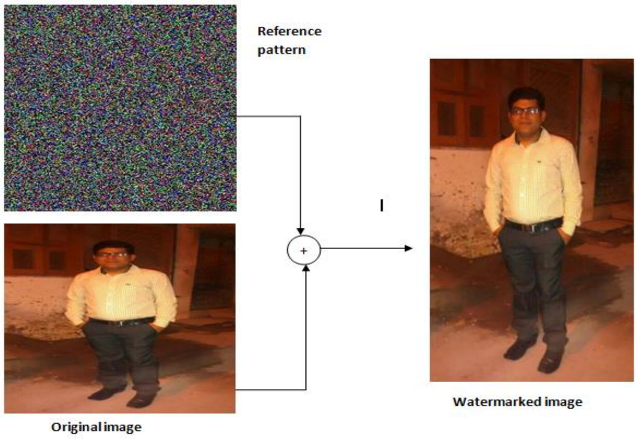

Fig. 2 Watermarking using blind embedding Technique

IV. Performance Assessment

In this work, simulation is using Matlab software to find the performance of blind embedding technique for watermarking. We are conducting three scenarios as following

A. Test-1

To examine the effectiveness of this system I have used 20 different images of same pixels (120 × 180 × 3 pixels). I took the α= 1 for embedding algorithm and embed a 1 and a 0 in each images. After doing this calculation for linear correlation for each image and for the original is also done. I have taken x-axis as linear correlation value and y-axis as percentage of images that have its own linear correlation value

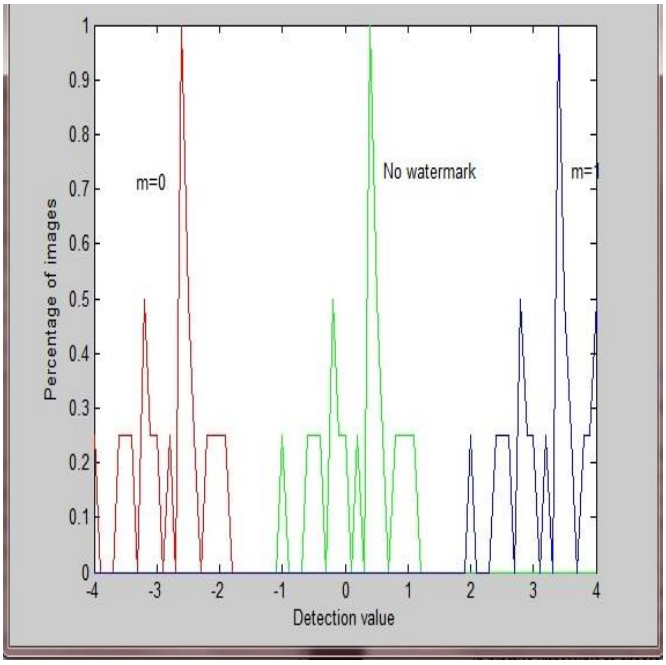

Fig. 3 Detection values for watermarked images test -1

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

As per result of watermark Images that has 0 embedded value lies on negative side. Images have a 1 embedded value lies on positive side. The un-watermarked images has a value and lies on 0. The value of threshold to be chosen is difficult to chose because there will be some un-watermarked images classified as watermarked images, this is called false positive and sometimes having watermarked images classified as un-watermarked images, this is called false negative.

B. Test-2

To analyze the performance of the system I have used 10 same images of pixels 120 × 180 × 3. I took the α= 1 for embedding algorithm and embed a 1 and a 0 in each images. After doing this calculation for linear correlation for each image and for the original is also done. I have taken x-axis as linear correlation value and y-axis as percentage of images that have its own linear correlation value.

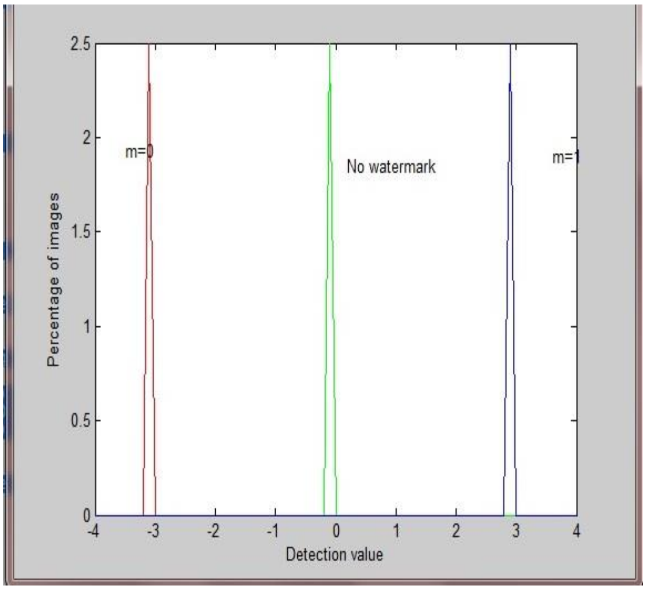

Fig. 4 detection values for watermarked image test-2

The x-axis is the linear correlation value and y –axis is the percentage of images having specific linear correlation function. The images having a 0 embedded had value centered on -3. Those that have a 1 embedded value centered on 3 and un-watermarked images had value centered on 0.

C. Test-3

Again for more enhancements I have used 200 images of same pixels 120 × 180 × 3. I took the α= 1 for embedding algorithm and embed a 1 and a 0 in each images. After doing this calculation for linear correlation for each image and for the original is also done. I have taken x-axis as linear correlation value and y-axis as percentage of images that have its own linear correlation value.

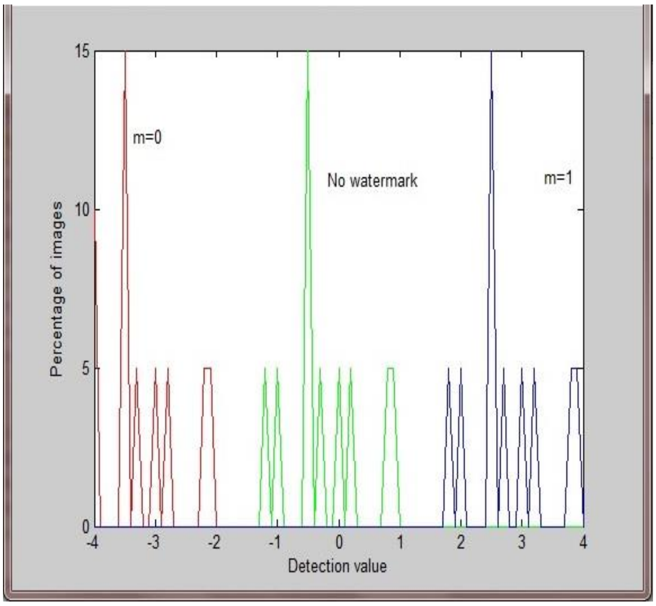

Fig. 5 detection values for watermarked images test-3

As the number of images increases the threshold value is not cleared as in figure 4. Again the Images that has a 0 embedded value lies on negative side. Images that has a 1 embedded values lies on positive side. The un-watermarked images has a value and lies on 0. The value of threshold to be chosen is difficult to chose because there will be some un-watermarked images classified as watermarked images, this is called false positive and sometimes having watermarked images classified as un-watermarked images, this is called false negative.

V. CONCLUSION

In this paper, simulate and analyze blind embedding and linear correlation technique. The digital watermarking technique is very stirring for image authentication or protection from piracy. The blind embedding and linear correlation detection is good for application where exact watermark need to be extracted and channel do not consist any noise then the exact threshold value be detected for watermarked images.

REFERENCES

1. Mei Jiansheng, Li Sukang and Tan Xiaomei "A Digital Watermarking Algorithm Based On DCT and DWT-"- WISA'09, Nanchang, P.R. China, May 22-24, 2009, pp. 104-107.
2. Shradha S. Katariya(Patni) "Digital Watermarking: Review", IJEIT, Volume 1, Issue 2, February 2012, pp. 143-153.
3. Mohan Durvey and Devshri Satyarthi "A Review Paper on Digital Watermarking" - IJETICS, Volume 3, Issue 4, July- August 2014, pp. 99-105.
4. Radhika v. Tola and K.S. Bapat, "Comparative Analysis of Watermarking in Digital Images Using DCT and DWT" International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013,pp. 1-4.
5. Keshav S. Rawat and Dheerendra S Tomar, "Digital Watermarking Schemes For Authorisation Against Copying Or Piracy Of Color Images", Indian Journal of Computer Science and Engineering, Volume 1, Number 4, pp. 295-300.
6. J. Anitha and S. Immanuel Alex Pandian, "A Color Image Digital Watermarking Scheme Based On SOFM" International Journal of Computer Science Issues, Volume 7, Issue 5, September 2010, pp. 302-309.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

7. DolleyShukla and Manisha Sharma, “Watermarking Schemes For Copy Protection: A Survey” International Journal of Computer Science and Engineering Services, volume 3, Number 1, February 2012, pp. 65-71.
8. Aseem Saxena, Amit Kumar Sinha, Shashank Chakarwarti and Surabhi Charu, “Digital Watermarking Using MATLAB” International Journal of Advances in Science Engineering and Technology, Volume 1, Issue 3, June 2014, pp. 39-42.
9. Karnpriya Vyas, Kriti Sethiya and Sonu Jain- “Implementation of Digital Watermarking Using MATLAB SoftwareCOMPUSOFT” An International Journal of Advanced Computer Technology, Volume 1, Issue 1,2012, pp. 1-7.
10. P. Ramana Reddy, V. N. K. Prasad and D. Sreenivasa Rao, “Robust Digital Watermarking of Color Images under Noise Attacks” - International Journal of Recent Trends in Engineering, Volume 1, Number 1, May 2009, pp. 334-338.
11. Er. Deepak Aggarwal, Er. Sandeep Kaur and Er. Anantdeep, “An Efficient Watermarking Algorithm to Improve Payload and Robustness without Affecting Image Perceptual Quality” Journal of Computing, Volume 2, Issue 4, April 2010, pp. 105-109.
12. P. Surekha and S. Sumathi, “Implementation of Genetic Algorithm for a DWT Based Image Watermarking Scheme” ICTACT Journal, Volume 2, Issue 1, July 2011, pp. 244-252.
13. Sajjad Bagheri Baba Ahmad, “Image Watermarking: Blind Linear Correlation Technique”TI Journals, World Applied Programming, Volume 5, Number 5, May 2015, pp. 93-100.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)