International Journal of Engineering Research ISSN: 2348-4039
& Management Technology
November-2015 Volume 2, Issue-6
Email: editor@ijermt.org www.ijermt.org

A STUDY OF ENTROPY BASED DIGITAL WATERMARKING

Ajay Kumar
Ph.D Scholar
Computer Engineering
NIILM University
Kaithal, Haryana

Dr. Pankaj Kumar Verma
Professor
Department of CSE
NIILM University
Kaithal, Haryana

1. INTRODUCTION:

The growth of high speed computer networks and World Wide internet (WWW) have explored means of latest business, scientific, diversion and social opportunities within the kind of electronic commercial enterprise and advertising, messaging, period data delivery, data sharing, collaboration among computers, product ordering, group action process, digital repositories and libraries, internet newspapers and magazines, network video and audio, personal communication and much additional. The price effectiveness of merchandising software within the kind of digital pictures and video sequences by transmission over computer network is greatly increased attributable to the improvement in technology.

We know that one amongst the largest technological events of the last 20 years was the invasion of digital media in a whole. Digital information may be stored expeditiously and with a really prime quality, and it may be manipulated terribly and simply by victimization computers. What is more, digital information may be transmitted in an exceedingly quick and cheap method through digital communication networks while not losing quality. Digital media provide many distinct blessings over analog media. The standard of digital audio, images and video signals is much better than that of their analog counterparts. Copying is easy because one can easily find out the exact discrete locations to be changed. Writing is straightforward as a result of one will access the actual separate locations that would like to be modified. Repetition is easy with no loss of fidelity. A duplicate of a digital media is clone of the first. With digital transmission distribution over World Wide Web, authentications are additional vulnerable due to the possibility of unlimited repetition. For digital information, copyright social control and content verification are terribly troublesome tasks. One answer would be to limit access to the information victimization by using some cryptography techniques. However, cryptography doesn't offer overall protection. Once the encrypted informations are decrypted, they can be freely distributed or manipulated. Unauthorized use of information creates many issues. As an example, if we tend to visit the web site http:\\www.wallpaper.com, we tend to observe that each one the wallpaper pictures are created by the house owners, which are their holding Right (HR). Any user will transfer the wallpapers. Now, consider that a user downloads {the pictures or the photographs} and posts those images (either after modifying or original) on his/her web site.

1.1 DATA HIDING:

There are several techniques for information hiding into digital media. They are used for several purposes as well as copyright protection. Two basic methods of information hiding are cryptography and steganography. Cryptography is a widely used method for protecting the digital content of the media. The concept of digital watermarking is derived from steganography. The term steganography means “cover writing” and cryptography means “secret writing”. [1].

1.2 STEGANOGRAPHY:

Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling.

Steganography deals with the methods of embedding information within any other medium (host or cowl medium) in an unperceivable way. All kinds of digital knowledge (still pictures, audio, video, text documents and transmission documents) are often used as a cover medium for info concealing. In steganography, the message is embedded into the digital media rather than encrypting it in such a way that nobody except the sender and the intended recipient can even realize that there is a hidden message. The digital media content, called the cover, can be determined by anybody; but, the message hidden in the cover can be detected by only the person having the actual key. Thus steganography actually relates to covering point-to-point communication between two parties. That's why steganography methods are usually not robust against modification of the data.

Thus, steganography is a region that is, additional or less, a Hide-&-Seek game. Some vital data or information is hidden into another medium. Knowledge or information that is hidden isn't encrypted also. The key issue in this type of system is that nobody ought to suspect that a particular medium is carrying any hidden information. By using steganography the objective is not to make it difficult to read the message as cryptography does, it is to hide the existence of the message in the first place possibly to protect the courier

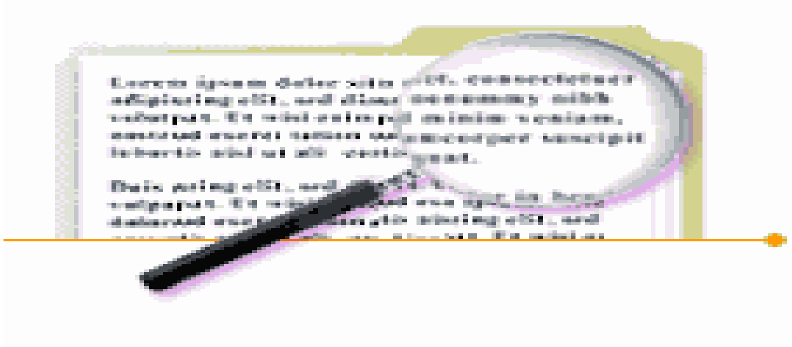

Figure 1: Securing Confidential data using Steganography

The stego media is similar to the cover media hence it is difficult for the hackers to detect the existence of secret message on the cover media. The hidden secret information can be extracted by retrieving algorithm. Two other technologies that are closely related to steganography are watermarking and fingerprinting. Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy.

1.3 WATERMARKING:

Watermarking is the process of computer-aided information hiding in a carrier signal. Watermarks may be used to verify the authenticity or the integrity of the carrier signal or to show the identity of its owner. It is prominently used for tracing copyright infringements and for banknote authentication. Watermarking tries to control the robustness at top priority This space of application of steganography is understood as Digital Watermarking. Digital watermark could be a message/data/information that is embedded into digital content (audio, video, images or text) which will be detected or extracted later. Such message/data/information principally carries the copyright or possession info of the content. The method of embedding digital watermark info into digital content is understood digital watermarking

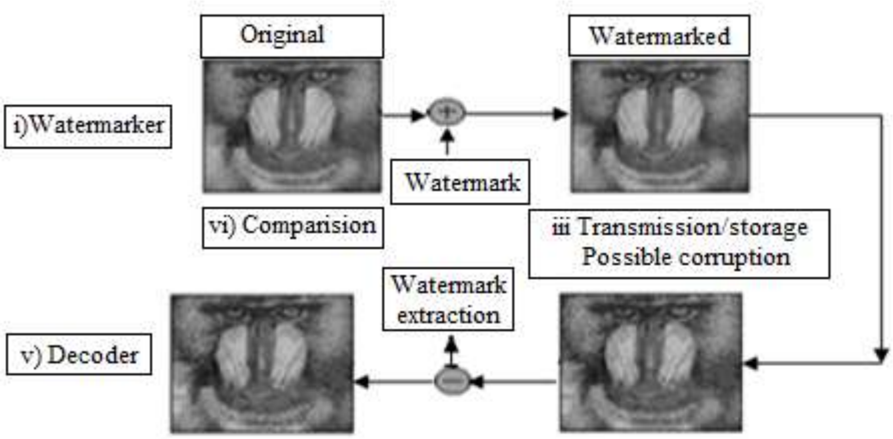

Figure 2: General watermarking scheme

Figure 3: Watermark on a bank currency note

1.4 DIGITAL WATERMARKING:

A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked

1.5 ENTROPY:

Entropy is a measurement of uncertainty, the area with large entropy keeps balance between robustness and transparency as a result. In information theory, **e**ntropy is a measure of the uncertainty in a random variable. Image entropy is a quantity which is used to describe the `business' of an image, i.e. the amount of information which must be present in the image. Low entropy images, such as those containing a lot of black sky, have very little contrast and are venerable to attacks. An image that is perfectly flat will have entropy of zero. Consequently, they can be compressed to a relatively small size.

In order to keep effectiveness of media content communication, the area with more information provides high robustness. For another, the area with great uncertainty provides excellent masking effect, leading to high transparency. While the entropy is a measurement of uncertainty, the area with large entropy keeps balance between robustness and transparency as a result. Formula to calculate the entropy value

$$Entropy = -\sum_i P_j Log_2 P_j \qquad (1)$$

In the above expression, P_i is the probability that the difference between 2 adjacent pixels is equal to i, and Log_2 is the base 2 logarithm.Entropy Filtration will return a value where each pixel contains the entropy value of the 9-by-9 neighborhood around the corresponding pixel in the output image.

2. LITERATURE REVIEW:

Juan R. Hernández et al. (2000) [2] proposed a spread-spectrum-like discrete cosine transform domain (DCT domain) watermarking technique for copyright protection of still digital images is analyzed. The DCT is applied in blocks of 8 × 8 pixels as in the JPEG algorithm. The watermark can encode information to track illegal misuses. For flexibility purposes, the original image is not necessary during the ownership verification process, so it must be modeled by noise. Two tests are involved in the ownership verification stage: watermark decoding, in which the message carried by the watermark is extracted, and watermark detection, which decides whether a given image contains a watermark generated with a certain key.

Marc Van Droogenbroeck et al. (2002) [3] proposes an entropy based technique for data embedding in images with a specific target, sometimes referred to as feature location: inclusion of a maximum amount of information instead of robustness against attacks. After an introduction, we analyze the error that results from a modification of the least significant bits. Then we describe our embedding technique. Finally we examine the upper bound of information that can be embedded in the least significant bits by means of our technique and we conclude.

Samir Kumar Bandyopadhyay et al. (2010) [10] proposed a technique for hiding the data of images has been proposed. The proposed method is used to hide an image file entirely with in another image file keeping two considerations in mind, which are Size and Degree of Security. At the source, the image that is to be hidden (target image) is encoded within another image (cover image). Firstly, the cover image and the target image can be of any size, which will be adjusted by our Resize function thereby, removing the size constraint. Secondly, for the security of transmission over network, only the final encrypted image.

Darshana Mistry et al.(2011) [11] proposed a Digital watermarking scheme where image or video is embedded information data within an insensible form for human visual system but in a way that protects from attacks such as common image processing techniques. Spatial domain (Least significant bit (LSB)) and transform domain (Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)) methods are used. DWT is best method because of using embedded zero tree wavelet image compression scheme and high frequency sub bands**.**

Qiu Yang et al. (2012) [12] introduces the entropy masking model in three different domains, and gives experiment report about utilizing spatial domain, DCT domain, and DWT domain entropy masking model in the similar watermarking system. In addition, we analyze the advantages and disadvantages of these models from the aspects of imperceptibility and robustness through our simulation experiment

K. Mccnakshi et al.(2014)[13] proposed a robust watermarking for still digital images based on Fast Walsh-Hadamard Transform (FWHT) and Singular Value Decomposition (SVD) using Zigzag scanning. After applying Fast Wash-Hadamard transform to the whole cover image, the Walsh-Hadamard coefficients are arranged in zigzag order and mapped into four quadrants Q1, Q2, Q3,Q4. These four quadrants represent different frequency bands from the lowest to highest. The quadrant Q1 again divided into non overlapping blocks and in it the highest entropy block is selected and Singular Value Decomposition is applied and the singular values of that block is modified with the singular values of the Fast-Walsh-Hadamard transform and results of the proposed method are found to be superior in terms of imperceptibility and robustness at the expense of increased computational complexity.

3. PROBLEM FORMULATION:

Security and capacity of watermark data are very important issues to be considered. A lot of research is going on to increase security and capacity. The problem statements consist of embedding the watermark in Bi-orthogonal 2-DWT wavelet coefficient of the image. The watermark image was to be made secure with the aid of watermarking.

4. NEED OF THE STUDY:

Watermarking is not a fully mature technology, lots of research is going on in this field, spatially to increase security and capacity of watermark data. Most of researchers try to increase the watermark capacity by compromising image quality, because there is a tradeoff among data rate, security and imperceptibility. But with our scheme we will be able to embed more number of watermark bits without affecting the imperceptibility of the cover image. Our watermarking technique use will use entropy based digital watermarking using 2-D biorthogonal wavelet in this a secret key is generated which increases the security of watermark Here, the entropy based method is proposed for invisible watermarking in still grey scale images using discrete wavelet transform and histogram equalization.

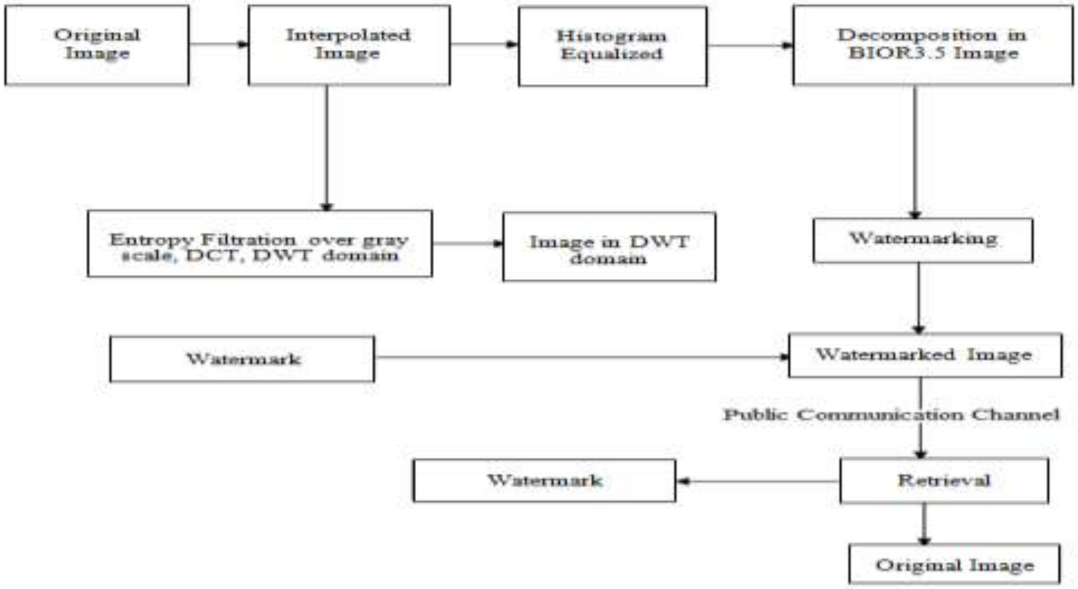

Figure 4: Formulation of Problem

5. PROPOSED WORK:

The proposed technique is based on interpolation, Entropy calculation, histogram equalization and Bi-orthogonal 2-DWT (discrete wavelet transform) domain. The original image is of 256*256 and watermark should be either equal to size of original image or less than that of the size of original image. The DWT domain improves the security and robustness during communication. The watermark is embedded into the DWT coefficients of the histogram equalized image. In our proposed system we first implement interpolation over the original image using bilinear interpolation; on the interpolated image we apply entropy filtration in order to find which domain is better for embedding the watermark. So we find that out of grey scale, DCT and DWT, DWT domain has highest entropy so for embedding DWT is chosen as it is more secure and less vulnerable to attacks and the PSNR(peak signal to noise ratio) of the DWT domain over the original image is higher than other domain and.

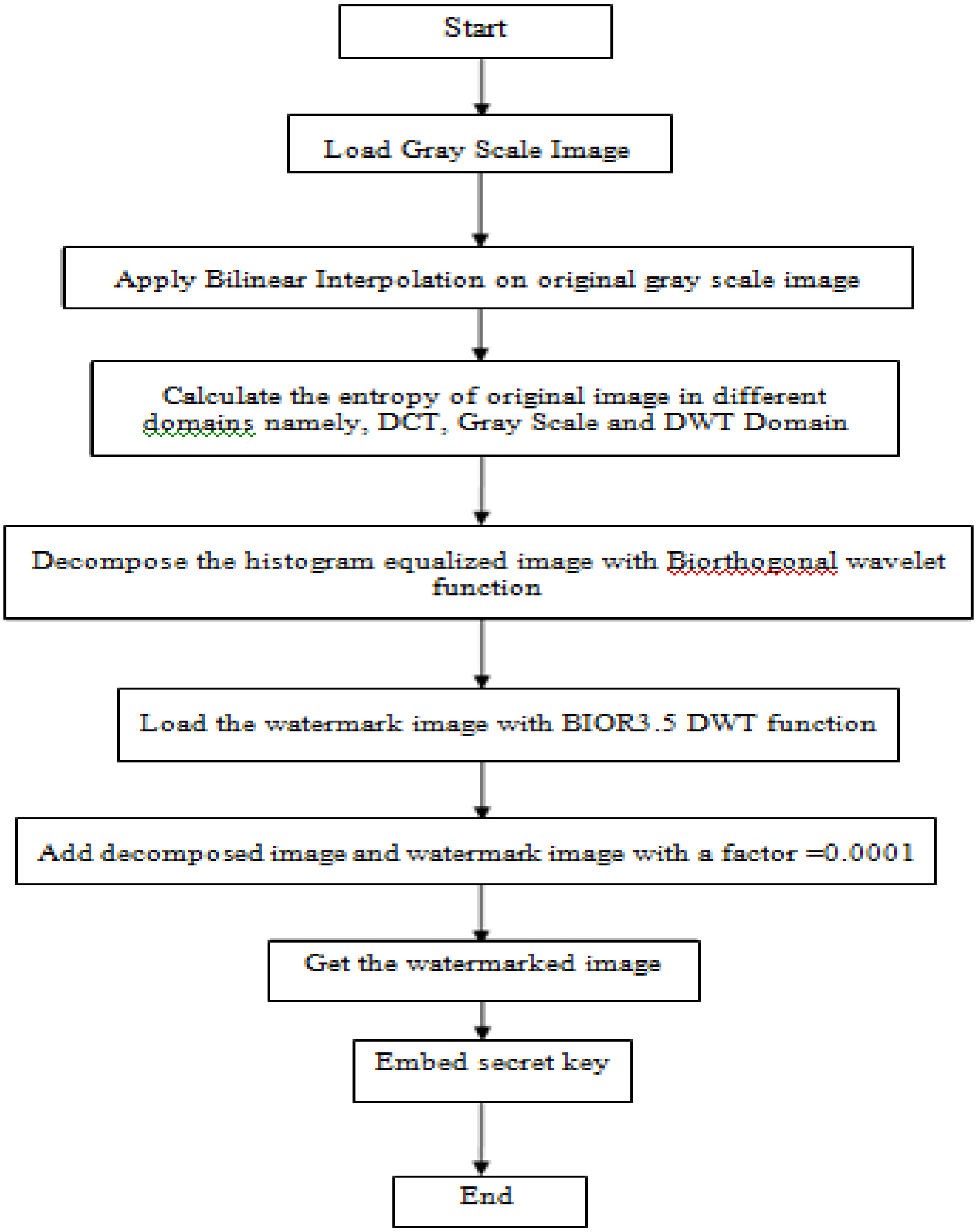
Start
Load Gray Scale Image
Apply Bilinear Interpolation on original gray scale image
Calculate the entropy of original image in different domains namely, DCT, Gray Scale and DWT Domain
Decompose the histogram equalized image with Biorthogonal wavelet function
Load the watermark image with BIOR3.5 DWT function
Add decomposed image and watermark image with a factor =0.0001
Get the watermarked image
Embed secret key
End

Figure 5: Steps of Proposed work to embed the watermark and to get the watermarked image

6. RESEARCH METHODOLOGY:

The watermark is embedded into original image by calculating entropy value so that we can find which area has maximum uncertainty or randomness in order to insert watermark so that it is invisible to others. While embedding we can first improve the quality of image and also remove the pixel errors based on bi-linear interpolation. Following Methods will be used for the implementation of the proposed work.

- **Interpolation image**
- **Entropy calculation**
- **Histogram equalized image**
- **Decomposition with (Biorthogonal-3.5) 2D-wavelet**
- **Watermark image**

7. CONCLUSION:

The watermarking is used to transfer copyright information over open channel. The technique proposed here is based on interpolation, histogram equalization, entropy filtration and Bior3.5 DWT. The number of MSBs of payload to be embedded in the cover image based on DCT coefficients. The original image is of 256*256 and converted into DWT coefficients for embedding process .The invisible watermark is added to the original image to make it more protected. The integrity of the data embedded in the original image retains. It is observed that the proposed techniques comes up with a good PSNR(Peak Signal to Noise Ratio), MSE(Mean square error) values and enhanced security and also the secret key by the user or authorized person is added and is used at another side when one want to extract the hidden data(watermark) from the original image. If anyhow the key entered by the user is wrong then user is not able to extract the watermark. Any intruder cannot find that there is some watermark is added into the original image and when trying he/she fails and would not be able to copy it or extract anything.

REFERENCES:

1. http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
2. Juan R. Hernández, Martín Amado & Fernando Pérez-González,” DCT-Domain Watermarking Techniques for Still Images Detector Performance Analysis and a New Structure”, IEEE trans, VOL. 9, NO. 1, January 2000.
3. Marc VAN DROOGENBROECK & Jérôme DELVAUX,” An entropy based based technique for information embedding in images ”, IEEE Benelux Signal Processing Symposium (SPS-2002), Leuven, Belgium, March 21–22, 2002.
4. A.K. Mikkilineni, G. N. Ali, P. J. Chiang, G. T. Chiu, J. P. Allebach & E. J. Delp, “Signature-embedding in printed documents for security and forensic applications”, in Proceedings of SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VI, vol. 5306, pp. 455-466,2004.
5. Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, & Wei Su,” Reversible Data Hiding”, IEEE trans, VOL. 16, NO. 3, MARCH 2006.
6. Po-Yueh Chen & Hung-Ju Lin,” A DWT Based Approach for Image Steganography”,IJASE trans,2006.
7. C. C. Lin and N. L. Hsueh, “A lossless data hiding scheme based on three-pixel block differences,” Pattern Recogni., vol. 41, no. 4, pp. 1415–1425, Apr. 2008.
8. Mehdi Boroumand and Afshin Ebrahimi,” An Improved Quantization Based Watermarking Scheme Using Local Entropy in Wavelet Domain”, IEEE International Conference on Signal and Image Processing Applications,2009.
9. P. Tsai, Y. C. Hu, and H. L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Process., vol. 89, pp. 1129–1143, 2009.
10. Samir Kumar Bandyopadhyay, Tuhin Utsab Paul & Avishek Raychoudhury,” An Encryption Based Technique for Invisible Digital Watermarking”, IJCA trans,2011.
11. Darshana Mistry,” Comparison of Digital Water Marking methods”, IJCSE trans, Vol. 02, No. 09, 2010.
12. Qiu Yang, Yana Zhang & Cheng Yang, Wei Li,” Information entropy used in digital watermarking”,IEEE trans,2012.
13. K.Mccnakshi,Ch.Srinivasa Rao, K.Satya Prasad” A Robust watermarking scheme based on Walsh-Hadamard Transform and SVD using Zig-ZagScanning”Master Thesis, and International Conference on Information Technology,2014.
14. Matrix laboratory help 12.0.