International Journal of Electrical Electronics & Computer Science Engineering
Volume 2, Issue 4 (August, 2015) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

# Watermarking Technique for Analysis of Security & Capacity of Watermark Data

Neelam Yadav[1], Jitender Yadav[2], S S Yadav[3]
[1]Scholar, Computer Science & Engg. Deptt., RPSGOI, Mahendergarh
[2]Assistant Professor, Computer Science & Engg. Deptt., RPSGOI, Mahendergarh
[3]Dean, PG Academics, Computer Science & Engg. Deptt., RPSGOI, Mahendergarh
[1]neelization@gmail.com, [2]jitendery006@gmail.com, [3]deanpg@rpsinstitutions.org

***Abstract:*** ***The recent years in the digital multimedia technologies has offered many facilities in the transmission, reproduction and manipulation of data. The advancement has also many challenges such as copyright protection for content providers. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. This technique is better than digital signatures and other methods because it does not increase overhead.***

***This dissertation, present a new watermarking technique that can embed multiple watermarks in the cover image without affecting the imperceptibility and increase the security of watermarks.***

***Keywords: Watermarking, Digital Watermarking, Framework, Digital Signatures.***

## I. INTRODUCTION

With the ever-growing expansion of digital multimedia data present on Internet has become increasingly popular. The advancement in technology has dual impact. As on one hand, it has enabled faster and more efficient storage, transfer and processing of digital data; on the other hand, duplication and manipulation of digital contents has also become very easy and undetectable.

Digital watermarking techniques used for protecting the multimedia data from copyright infringement. "Digital watermarking can be defined as a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm."

This kind of watermark contains the author and the user's information, which could be the owner's logo, serial number or control information. Digital watermarking is very common in everyday lives; watermarking in currency, government documents, stamps and many other common documents. The main use of watermarking is to provide a level of certainty about the authenticity and ownership of a document.

## II. APPROACH

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, a dark background), caused by thickness or density variations in the paper. There are two main ways of producing watermarks in paper; the dandy roll process and complex cylinder mould process. Watermarks are often used as security features of bank notes, passports, postage stamps and other documents. Watermark is very useful in the examination paper because it can be used for dating, identifying sizes, mill trademarks and locations, and the quality of a paper.

## III. GENERAL FRAMEWORK

Digital watermarking is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format.

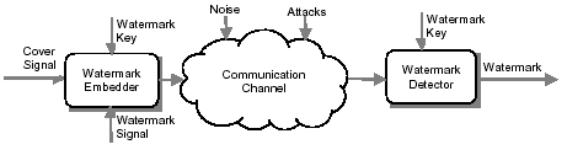


Fig 1: Generic Digital Watermark Embedding and Detection Scheme

## IV. COMPARISON OF WATERMARKING WITH DIGITAL SIGNATURES

In watermarking embed metadata into the multimedia content directly in such a way that not required additional bandwidth. Historically, integrity and authenticity of digital data has been guaranteed through the use of digital signatures. In that case use header part of the document for signature embedding. So additional bandwidth is required, which increase overhead.

## V. IMPLEMENTATION DETAILS AND EXPERIMENTAL RESULTS

In this dissertation, a new image watermarking method is implemented. This method increases the security and

International Journal of Electrical Electronics & Computer Science Engineering
Volume 2, Issue 4 (August, 2015) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

capacity of robust watermark. To increase capacity the concepts of multiple text files are used i.e. to embed multiple data files in the image and to increase security by encryption embedding invisible watermark.

In this proposed system watermark is embedded at high frequencies using watermarking method at frequency domain so that both objectives of efficiency and reliability are effectively controlled and achieved which gives the proposed system more security and efficient. Inverse mode of watermarking method extracts the data from the image without any kind of data loss.

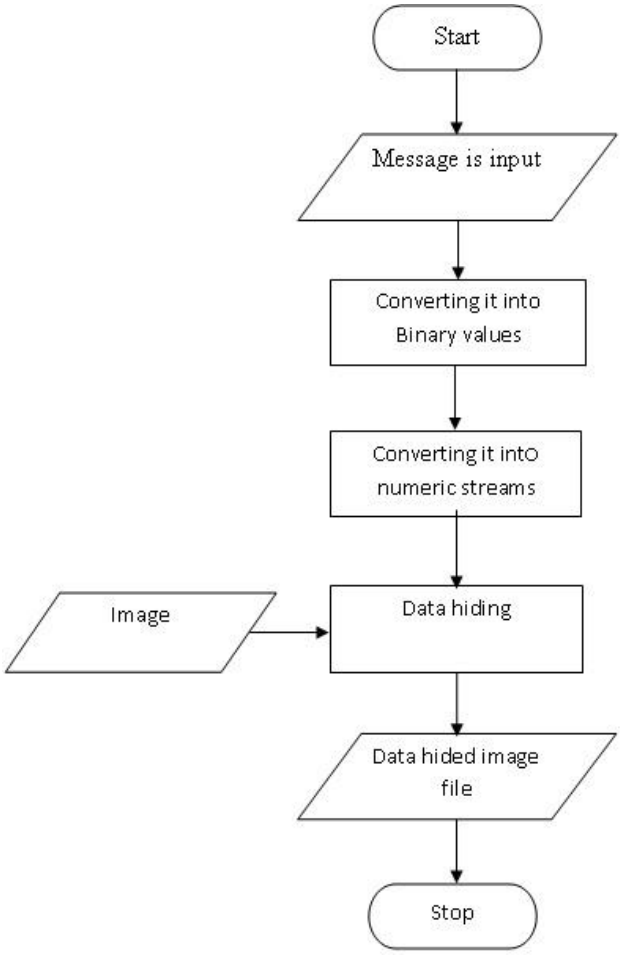


Fig:2 Steps of Embedding Process of Watermarking

For embedding watermark divide the complete image in different segments based on the frequency ratio in different image areas. Categorize this image from low to high frequency area. Each segment is represented by the separate matrix. The size of the matrix depends on two factors. One is the intensity level in that area it means all the pixels of same intensity in one segment represents one frequency area. Another factor is the data size. To store the data in an image divide the complete data in the form of a matrix then this matrix is placed on this segmented area matrix and the correlation is performed between these two matrices in order to hide the data behind the image. Each sub image will be processed separately according the proposed approach. The selection of the image segment is done on the random basis. It means first, any image area is selected randomly to work on it. After this on this image area the frequency domain is processed in order to identify different image segments. A search is performed to identify the segment respective to that random point. All the surrounding pixels are processed and their frequency values are calculated. After this all the same frequency pixels are kept in one domain and as the result a frequency segment is been selected and defined.

*Embedding Process*

In the system defined in fig. 2first work is to get the input text and the source image. After this the stored data will be converted to the raw data format that represents bit system. Now the actual watermarking approach will be defined to hide data over the image. Finally, get the output watermarked image.

*Data Conversion*

In data conversion module the given data is converted into its binary values and those binary values are changed into numeric streams because if a hacker try to get the data behind the image it cannot be understandable to him this process makes the project more secured. Data conversion is explained with the help of fig. 3 which is given below:

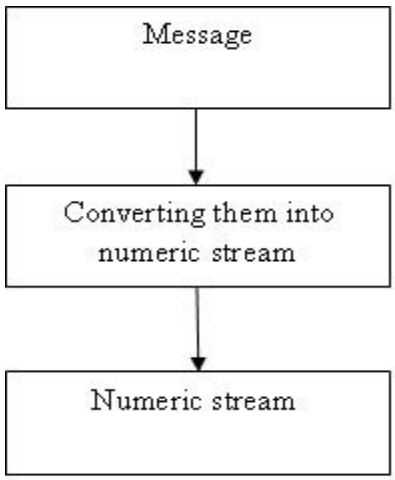


Fig: 3 Steps of Data Conversion in Embedding Process

*Watermarking*

This is the module for embedding process, in this module we are going to watermark the data from the above

International Journal of Electrical Electronics & Computer Science Engineering
Volume 2, Issue 4 (August, 2015) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

module in the given Microsoft word document this process is done by converting the word document into bytes and combining the data from the above module in the word document the output is a watermarked word document.

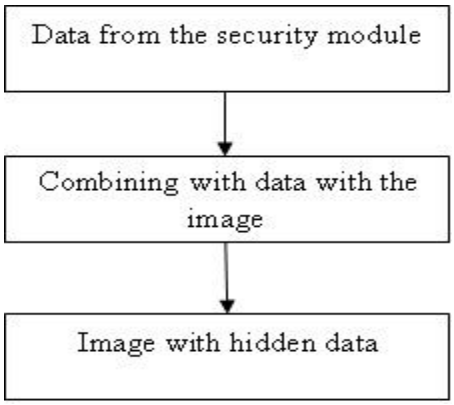


Fig: 4 Embedding Watermark into Image

*Extraction Process*

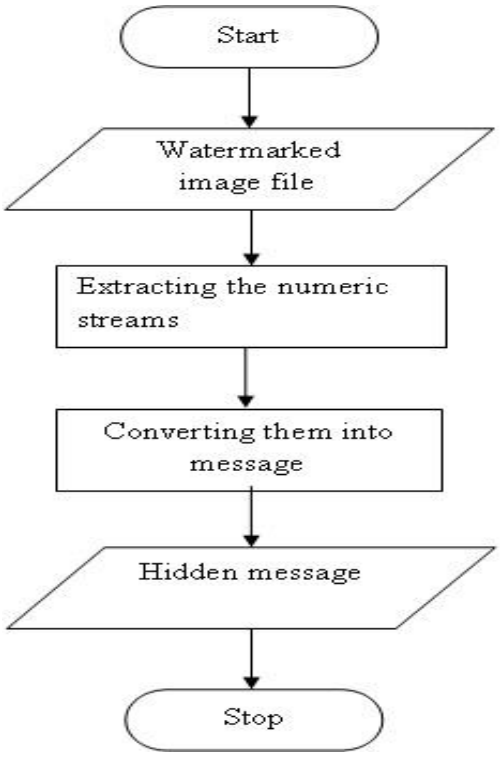


Fig: 5 Extraction Process of Watermark from Watermarked Image

It is the last module in this project. In this module input is image with data hidden inside and the hidden data is extracted by giving a correct key. The extracted data will be in the form of numeric stream so they are converted into binary values and using those binary values, the data is formed. In this extraction process the first work is to extract the watermarked image. Now perform the algorithm in reverse order to scan it and to retrieve the data back. Once the data is retrieved in binary format the will be stored to the specified location.

## VI. EXPERIMENTAL RESULTS

In experimental results, images of different sizes are used. These Images are shown are shown as source image. Measure the quality of watermarked images in terms of PSNR (Peak Signal to Noise Ratio). The less the value of PSNR, the more perceptible the watermark is. Histograms are used to show difference between source image and watermarked image.

In fig.5 source image and embedded image are shown. Source image is indicated by original image and embedded image is indicated by watermarked image. In this figure several options are shown, for performing watermarking, invisible watermarked option is used and for extracting watermark from embedded image 'get back hidden files' option is used.

Fig: 6 Framework for Embedding and Extraction of Watermark

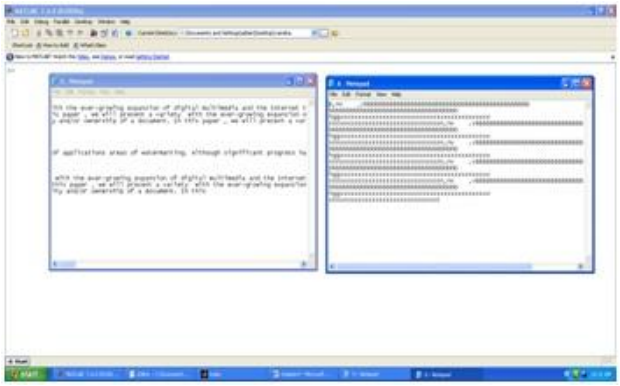

Fig: 7 Watermarks as Text Files (Watermark1 and Watermark2)

## VII. HISTOGRAMS RESULTS

An image histogram is a type of histogram that acts as a graphical representation of the tonal distribution in an image. It plots the number of pixels for each tonal value.

International Journal of Electrical Electronics & Computer Science Engineering
Volume 2, Issue 4 (August, 2015) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance. The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone. Two histograms are generated, one for source image and another for watermarked image. Histograms are showing frequency components of pictures. There are very minor differences in both source image histogram and watermarked image histograms because watermark is embedded at LSB of high frequency components or coefficients. Fig 8 shows histogram for source image and Fig. 9 shows histogram for watermarked image.

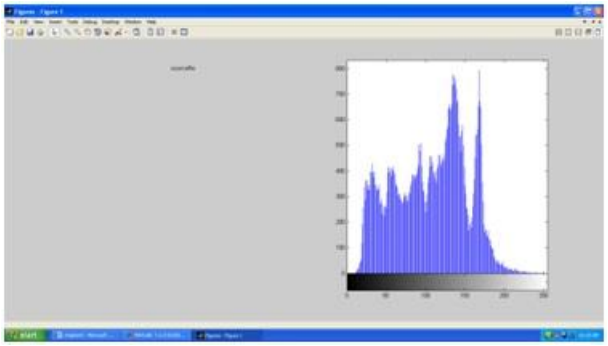

Fig: 8 Histogram for Source Image

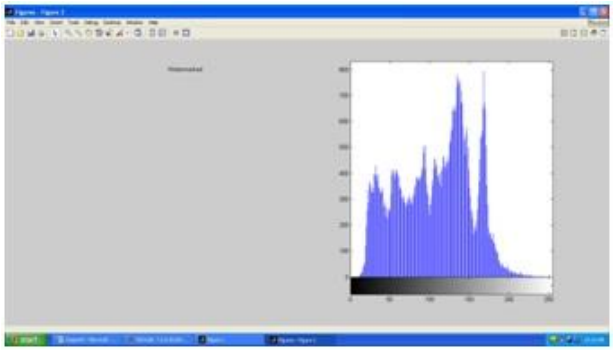

Fig: 9 Histogram for Watermarks Image

## VIII. CONCLUSIONS

The proposed invisible watermarking system is secure as the data is stored in different segments of the images randomly. There is no static area to store data in image. Such as in case of LSB data is stored from the initial of the image byte by byte. But in this work area will be selected dynamically by the proposed system itself. The proposed system is efficient. The proposed system is easy to understand with basic knowledge of the matrix system. Typically proposed technique is computationally pricey, and unpredictable. This remains one of the major problems in the development of robust digital watermarking for digital images Even if the algorithm is know it is not easy to retrieve the data. Before embedding encrypted both the watermarks with exclusive OR (XOR) operation. This provides an additional level of security for watermarks. For instance if watermarking key is hacked still the attacker will not be able to identify the watermark because it is encrypted.

## IX. SCOPE OF FUTURE WORK

Watermarking is an emerging research area for copyright protection and authentication of electronic documents and media. Most of the research is going on in this field; the reason might be that there are so many images available at Internet without any cost, which needs to be protected. The watermarking technique that is given in this dissertation can be further extended by incorporating a public private key combination to store the data with authenticity.

In future, work may be extended on different media like video, audio etc by using this approach. Right now the proposed approach is working only with the images.

In this technique used encryption is based on XOR operation. So, further work can be done to find some other encryption technique to increase the security of Watermarks.

## X. REFERENCES

[1] A. K. Vanwasi, “Digital Watermarking-Steering the Future of Security” Network Magazine, Indian Enterprise Group, Mumbai Edition 2001.

[2] Athanasios Nikolaidis and Ioannis Pitas,”Region-Based Image Watermarking” IEEE Transaction On Image Processing, Vol.10, No.11, PP. 1726 – 1740, 2001.

[3] Jiang Du, Choong-Hoon Lee, Heung-Kyu Lee, Youngho Suh,”BSS: A New Approach for Watermark Attack” MSE, IEEE Fourth International Symposium on Multimedia Software Engineering(MSE 02), PP. 182-187, 2002.

[4] Christian S. Collberg, Member and Clark Thomborson, ”Watermarking, Tamper-Proofing, and Obfuscation Tools for Software Protection” IEEE Transactions on Software Engineering, Vol. 28, No. 8, PP. 735-746, 2002.

[5] FrankY. Shih, Scott Y.T. Wu,”Combinational image watermarking in the spatial and frequency domains” Science Direct, Vol. 36, No. 4, PP. 969-975, 2003.

[6] Mauro Barni, Franco Bartolini, Alessia De Rosa, and Alessandro Piva,”Optimum Decoding and Detection of Multiplicative Watermarks” IEEE Transaction On

Signal Processing, Vol. 51, No. 4, PP. 1118-1123, 2003.

[7] Yongjian Hu, Sam Kwong and Jiwu Huang,"Using Invisible Watermarks to Protect Visibly Watermarked Images" Vol.5, PP. 584-587, IEEE, 2004.

[8] Ping Dong, Jovan G. Brankov, Nikolas P. Galatsanos, Yongyi Yang, Franck Davoine,"Digital Watermarking Robust to Geometric Distortions" IEEE Transactions on Image Processing, Vol. 14, No. 12, PP. 2140 – 2150, 2005.

[9] Khaled Mahmoud, Sekharjit Datta, and James Flint," Frequency Domain Watermarking: An Overview" The International Arab Journal of Information Technology, Vol. 2, No. 1, PP.33-47, 2005.

[10] Kamran Hameed, Adeel Mumtaz, and S.A.M. Gilani,"Digital Image Watermarking in the Wavelet Transform Domain" World Academy of Science, Engineering and Technology, Vol.13, PP. 86-89, 2006.