A Secure Data Transmission Scheme Based on Digital Watermarking (Image + Text)

Mr. Jagtap. D. V., Mr. M. M. Mukhedkar.

Abstract— **Now days, internet resulted in an considerable growth in multimedia applications. The explosive advancement of internet has made it easier to send the data/image accurate and faster to the destination. Besides this, it is easier to modify and misuse the valuable information through hacking at the same time. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. A watermark is a technique, image or text is impressed onto the another image, which provides evidence of its authenticity. Here an invisible watermarking technique (least significant bit) and a visible watermarking technique is implemented.**

This paper presents the general overview of image and text watermarking and different security issues such as ambiguity attack, cryptographic attacks etc. Various attacks such as ambiguity attack, cryptographic attacks etc. are also performed on watermarked images and their impact on quality of images is supplementary of paper. In paper, Image Watermarking using Least Significant Bit (LSB) algorithm has been used for embedding the message/ into the image. This work has been implemented through MATLAB.

Keywords - Watermarking, Least Significant Bit (LSB), Discrete Cosine Transform(DCT), MATLAB.

I. INTRODUCTION

This template, Watermarking is a technique used to hide data or identifying information within multimedia. This paper will focus primarily on the watermarking of digital images. Digital watermarking is becoming famous, especially for adding undetectable marks, such as author or copyright information. Digital watermarking is a process to embed some information called watermark into different kinds of media called Cover Work [10]. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the another third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, and interpret the signal but protect the ownership of the original content. Digital watermarks are inside the information so that ownership of the information cannot be claimed by third party [8]. While some watermarks are visible [5], most watermarks are invisible.

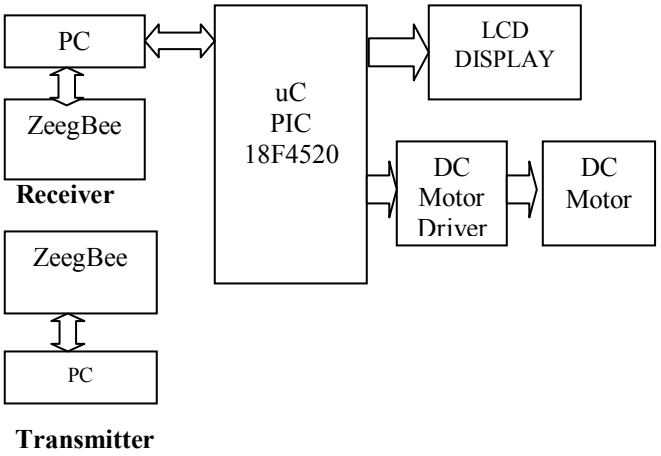
II. LITERATURE REVIEW

During the past ten years, digital watermarking has attracted the attention of numerous researchers. As a result, hundreds of studies have been published concerning the different methods for watermarking. The information embedded as a watermark can be almost anything. It can be a bit string representing copyright message, serial number, plain text, etc. However,
Sometimes it can be more useful to embed a visual watermark (e.g. corporate logo) instead of a bit string as a watermark.
The watermarking technique is used for data hiding. The main aspects of information hiding are capacity, security and robustness. Watermark can be divided into different types depending on applications. Many digital watermarking schemes have been proposed for still images and videos.

Most watermarking research and publications are focused on images. The reason might be that there is a large demand for image watermarking products due to the fact that there are so many images available at no cost on the World Wide Web which need to be protected. Meanwhile, the number of image watermarking publications is too large to give a complete survey over all proposed techniques. However, most techniques share common principles. Thus, we try to point out the common ideas first, before we explain some selected methods in more detail to illustrate how the principles are applied in practice. The watermark signal is typically a pseudorandom signal with low amplitude, compared to the image amplitude, and usually with spatial distribution of one information (i.e., watermark) bit over many pixels. A lot of watermarking methods are in fact very similar and differ only in parts or single aspects of the three topics: signal design; embedding; and recovery. The information that is embedded is usually not important for the watermarking itself. However, there are methods that are designed to embed and extract one out of a codebook of codes, and thus cannot accommodate arbitrary information.

 All Rights Reserved © 2014 IJARCET

III. BLOCK DIAGRAM-



IV. BLOCK DIAGRAM DISCRIPTION-

Digital Watermarking is a technique through which information or data is hidden or embed on to the image called Digital Watermarking.

In this project data is two co-ordinate X and Y angles for example 045° and 120°. This co-ordinate is embedded in image using MATLAB coding. Then that Watermarked image is being transmitted by using ZigBee. And technique used in watermarking is LSB(Least Significant Bit). We are using Watermarking scheme to avoid different type of attacks which does by hackers for extracting the information (data).

At Receiver end, using ZigBee receives the watermarked Image. Then using decreption technique we separate the information and image. That information i.e co-ordinate is interface to microcontroller through RS232. The LCD display will display the value of that co-ordinate whatever we give at the transmitter side. DC motor driver is interface through RS232. A missile model is connected to DC motor, that missile will rotate according to co-ordite values.

V. TECHNIQUES OF WATERMARKING

A. *Frequency Domain Watermarking*-
These methods are similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling of image, the watermark signal is applied to lower frequencies, or applied adaptively to frequencies containing important elements of the original picture.[4]

B. *Spread Spectrum*-
This technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the watermark extraction is possible without using the original unmarked image [1].

C. *Spatial Domain Techniques*-
Spatial domain class generally have the following characteristics:

- The watermark can applied in the pixel domain.
- No transforms are applied to the original signal during watermark embedding.
- Combination with the original or host signal is based on simple operations, in the pixel domain.
- The watermark can be identify or detected by correlating the expected pattern with the received signal.

Spatial domain watermarking is performed by modifying values of pixel color samples of a video frame. Let us denote a picture to be watermarked by P and values of its pixel color samples by Pi , a watermarked version of picture P by P * and values of its pixel color samples by P * i . Let us have as many elements of watermark W with values Wi as number of pixels in picture P1. Watermark W hereby covers the whole picture P1. Further, it is possible to increase the watermark strength by multiplying watermark element values by weight factor 'a'. Then the natural Formula for Embedding Watermark W into Picture P is: $P^*i = P\,i + aWi$

The most popular and common algorithm using spatial domain watermarking is LSB.

VI. LEAST SIGNIFICANT BIT

There are many algorithms available for invisible digital watermarking. The most common algorithm is Least Significant Bit (LSB) Insertion,4in which each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. [9]Given the extraordinarily high channel capacity of using the entire cover for transmission in same method, a small objects may be embedded many times.[9].In a digital image, information can be embedded directly into every bit of image information or the most busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image .Two techniques were presented to hide data in the spatial domain of images by it. These methods were based on the pixel value's of Least Significant Bit (LSB) modifications.

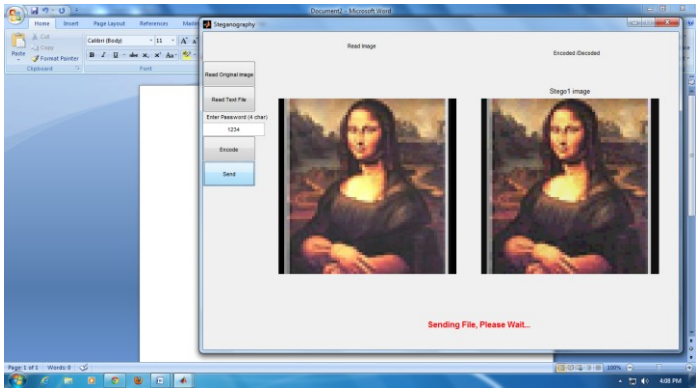
 All Rights Reserved © 2014 IJARCET

VII. STEPS OF LEAST SIGNIFICANT BIT

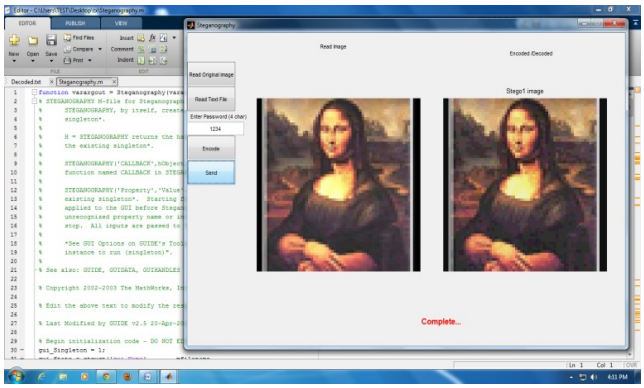
- Convert RGB image to gray scale image.
- Make double precision for image.
- Shift most significant bits to low significant bits of watermark image.
- Make least significant bits of host image to zero
- Add shifted version (step 3) of watermarked image to modified (step 4) host image.

VIII. RESULT

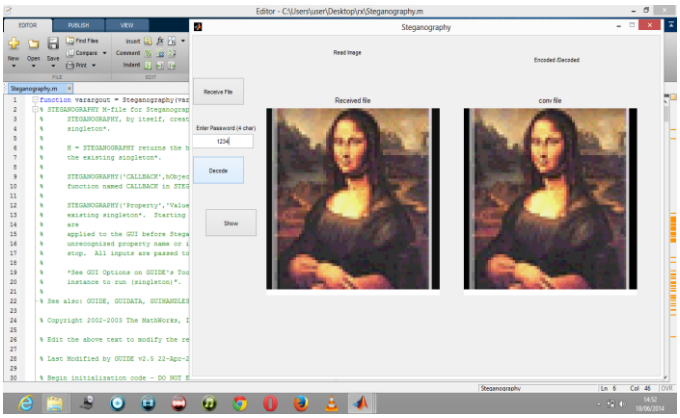
A. The screen of sending watermarked Image-



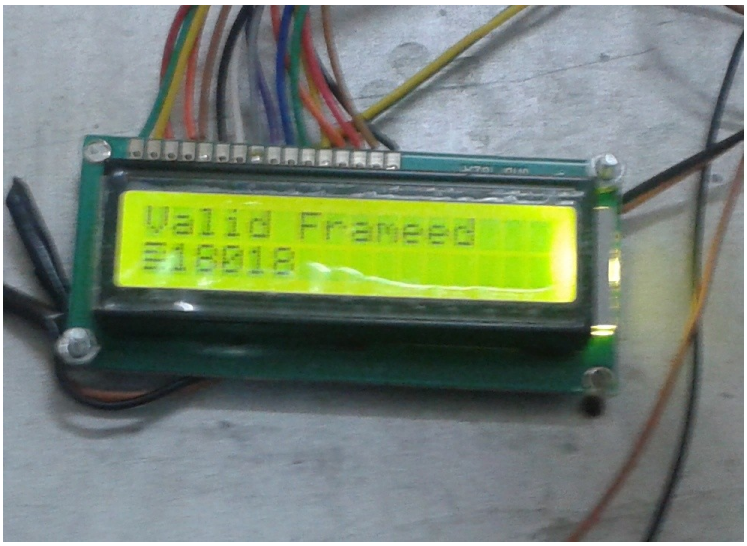
B. Watermarked Image at Transmitter side-



C. Original Image at Receiver side-



D. LCD showing Values of Co-ordinate (Text) –



IX. CONCLUSIONS

There are different techniques used in watermarking for security of images. Frequency domain, Spatial domain and spread spectrum. In this paper we use spatial domain method LSB for security of images, which is easy and simple and more effective method. Process of LSB is simple when we used LSB in MATLAB. A different image in MATLAB tells different process steps and their result. In future LSB may also use for other type of data and test on different type of images.

 All Rights Reserved © 2014 IJARCET

REFERENCES

[1] Avani Bhatia, Mrs. Raj Kumari "Digital Watermarking Techniques".

[2] B Surekha, Dr GN Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011

[3] Brigitte Jellinek, "Invisible Watermarking of Digital Images for Copyright Protection" University Salzburg, pp. 9 – 17, Jan 2000.

[4] Chiou- Ting Hsu; Ja-Ling Wu; Consumer Electronics "DCT-based watermarking for video", IEEE Transactions on Volume 44, Issue 1, Feb. 1998 Page(s):206 – 216

[5] Cox, Miller and Bloom, "Digital watermarking", 1st edition 2001, San Fransisco: Morgan Kaufmann Publisher

[6] Darshana Mistry "Comparison of Digital Water Marking methods"(IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 2905-2909

[7] Dr. Martin Kutter and Dr. Frederic Jordan, "Digital Watermarking Technology", Alp Vision, Switzerland, pp 1 – 4M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, International Journal of Modelling and Simulation, 18(2), 1998, 112-116.

[8] H. Arafat Ali, "Qualitative Spatial Image Data Hiding for Secure Data Transmission", GVIP Journal, Volume 7,Issue 2 , pages 35- 37, 2, August 2007

[9] Max Sobell "LSB Digital Watermarking", CPE 462

[10] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518.

[11] R.AARTHI, 2V. JAGANYA, &3S.POONKUNTRAN "Modified Lsb Watermarking For Image Authentication" International Journal of Computer & Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012 [12] 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.

[13] Yeuan-Kuen Lee1, Graeme Bell2, Shih-Yu Huang1, Ran-Zan Wang3, And Shyong-JianShyu "An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding" Springer-Verlag Berlin Heidelberg 2009.

Mr. Jagtap. D. V.
Elec. & Telecommunication Department
Dr.D.Y.Patil College Of Engineering, Ambi.
Pune India.

Mr. M.M Mukhedkar
Elec. & Telecommunication Department
Dr.D.Y.Patil College Of Engineering, Ambi.
Pune India.

 All Rights Reserved © 2014 IJARCET