Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.419 – 426

RESEARCH ARTICLE

Use of Watermarking Technique for Secured Transmission

Ms. Nidhi Bux[1], Prof. Kashiram. Jayaram. Satao[2]

Rungta College of Engineering & Technology, Kohka - Kurud Road, Bhilai - 490 024, Chhattisgarh, INDIA

nidhi21_2005@rediffmail.com

kjsatao@gmail.com

Abstract: - The necessity of fast and secured transmission of images is a daily routine and is necessary to find an efficient way to transmit over the network .This paper presents the general overview of image watermarking and different security issues for protecting the images from attacks that combines Encryption, Watermarking technique which is based on least significant bits (LSB) substitution method for safe image transmission purpose.

This paper presents the general overview of image watermarking and different security issues, various attacks are also performed on watermarked images and their impact on quality of images is also studied. In this paper, Image Watermarking using Least Significant Bit (LSB) algorithm has been used for embedding the message/logo into the image and we are checking for different noise attacks and evaluate PSNR and MSE values are for each noise attacks, and the noise attack which is having higher PSNR value and lower MSE value will give better and more clean image.

Keywords: - Watermarking, Least Significant Bit (LSB), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE).

I. INTRODUCTION

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light [2]. Watermarks are useful as security features of banknotes, passports, postage stamps and also in the examination papers. Encoding an identifying code into digitized music, video, images or other files is known as a **DIGITAL WATERMARKING** [4].

Digital Watermarking techniques can be classified as:

- Text Watermarking
- Image Watermarking
- Audio Watermarking
- Video Watermarking

The image watermarking algorithms can be classified into two categories: spatial-domain techniques (spatial watermarks) and frequency-domain techniques (spectral watermarks) [4]. The simplest spatial-domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of some randomly selected pixels. The spatial-domain techniques directly modify the intensities or color values of some selected pixels [5].

II. PROCESS OF WATERMARKING

The process of watermarking begins when the encoder inserts watermark into image, producing watermarked image. The decoder extracts and validates the presence of watermarked input or unmarked input[5]. If the watermark is visible, the decoder is not needed. Otherwise, the decoder may or may not require a copy of decoder to do this job. If input image and/or watermarked image are used, the watermarking system is called a private or restricted-key system; otherwise, the system is public or unrestricted-key system [1].

The decoder is so designed to process both marked as well as unmarked image. Finally, the decoder needs to correlate the extracted watermark with original image and compare the result to a predefined threshold that sets the degree of similarity accepted as a match [2]. If the correlation matches the threshold value, then watermark is detected i.e. original image belong to the user otherwise the data does not belong to the user.

The watermark embedded inserts a watermark onto the cover image and the watermark detector detects the presence of watermark information/logo. Sometime a watermark key is also used during the process of embedding and detecting watermarks. The watermark key has a one-to-one relation with watermark information. The watermark key is private and known to only intender users and it ensures that only desirable set of users can detect the watermark [3].
Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital image watermarking techniques should be resilient to both noise and security attacks[7].

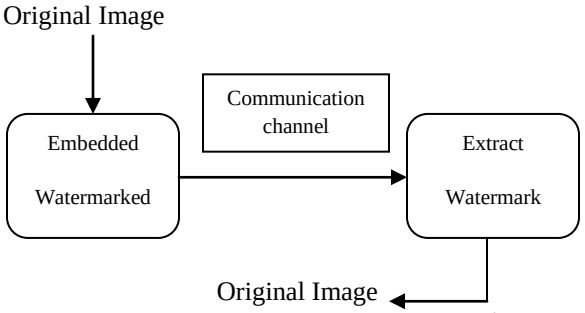

Fig 1. Process of Watermarking

III. METHODOLOGY

Based on LSB technique we propose a new watermarking technique for secured transmission of images, In this paper first we input an image which is a original image in which we embed watermark in the image (invisible watermark) with the LSB embedding algorithm, and we got a Watermarked Image without noticeable distortion on it, while the large watermark was recovered perfectly, in which we add distortion or noise attacks to the image to encrypt it, and then we got the encrypted image with different noise attacks. In the distorted image we calculate the Peak Signal to Noise Ratio (PSNR) & Mean Square Error (MSE) values for each noise attacks and compare whose PSNR value is higher it will give effective noise to images and MSE value is lower, The lower the value of MSE, the lower will be the error.

Noise recovery is done to remove noise of an image and the pixels are easily identified as noisy pixels in grayscale image but it is difficult to recognize in RGB color image [3]. Reason behind it is that, any color combination with white (pixel on) or black (pixel off) generate other color. The pixels are easily identified as noisy pixels in grayscale image but it is difficult to recognize in RGB color image. Reason behind it is that, any color combination with white (pixel on) or black (pixel off) generate other color. For noisy color image, convert it into grayscale and remove noise using noise removal **Random Function Selection Approximation Technique (RFSAT)**.

Water marking Extraction process is done to extract the watermark from the image through the process of watermarking begins when the encoder inserts watermark into image, producing watermarked image. The decoder extracts and validates the presence of watermarked input or unmarked input. If the watermark is visible, the decoder is not needed. Otherwise, the decoder may or may not require a copy of decoder to do this job. If input image and/or watermarked image are used, the watermarking system is called a private or restricted-key system; otherwise, the system is public or unrestricted-key system.

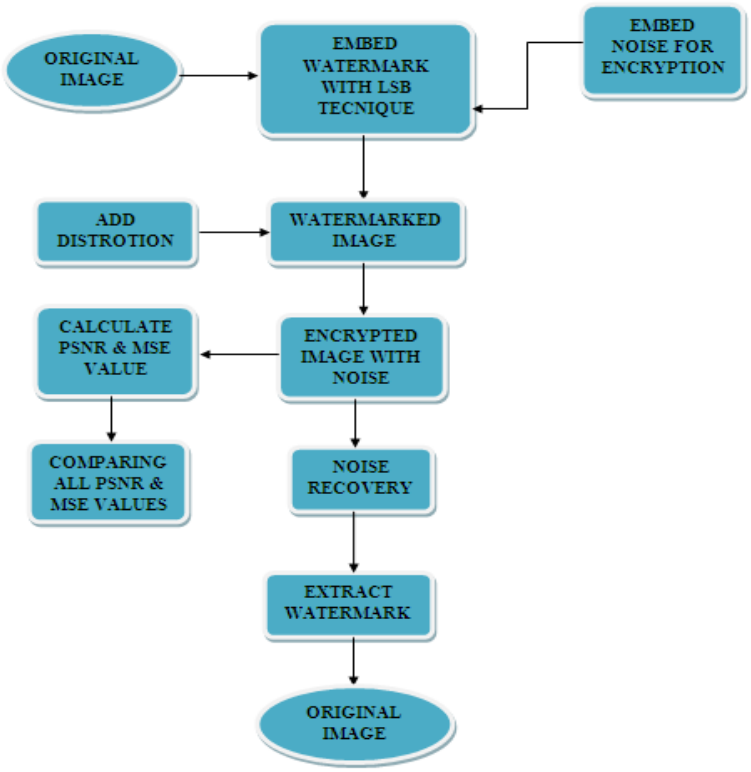

Fig 2. Block Diagram

A. Least Significant Bit Modification (LSB):-

The most straight-forward method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object. Despite of its simplicity, LSB substitution suffers from many drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the Watermark [8]. An even better attack would be to simply set the LSB bits of each pixel to one, fully defeating the Watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party [5].

After we have embedded the secret data in the first bit i.e. LSB in the image we got Watermarked Image without noticeable distortion on it. However when we embed the data in the consequent bits i.e. second towards last MSB bit, the image start distorted. An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key [6]. Security of the watermark would be improved as the Watermark could no longer be easily viewed by intermediate parties. The algorithm however would still be vulnerable to replacing the LSB's with a constant.

Method	PSNR	MSE
LSB or 1st Bit Substitution	55.8784	0.1680
2nd Bit Substitution	49.7986	0.6811
3rd Bit Substitution	43.9396	2.6249
4thBit Substitution	37.8535	10.6593
5thBit Substitution	31.9717	41.2961

6th Bit Substitution	26.0475	161.5588
7th Bit Substitution	26.0475	679.0598
MSB or 8th Bit Substitution	14.3467	2.3900e+003

TABLE 1. PSNR & MSE for Different Bit Substitution.

B. Images with Distortions

We have applied different types of distortions to the watermarked image so that no one (hacker) can hack our original image. There are different types of distortions/noise which we can apply into the images and send it to the receiver.

Fig 3. Watermarked Image

Various attacks in watermarked image:-

- Gaussian noise
- Poisson noise
- Speckle noise
- Gaussian Blur

1. *Gaussian Noise:-*

Gaussian noise is statistical noise that has its probability density function equal to that of the normal distribution, which is also known as the Gaussian distribution.

GAUSSIAN NOISE

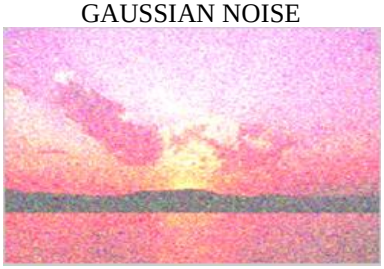

Fig 4. Gaussian Noise

2. *Poisson Noise:-*

Poisson noise or shot noise is a type of electronic noise that occurs when the finite number of particles that carry energy, such as electrons in an electronic circuit or photons in an optical device, is small enough to give rise to detectable statistical fluctuations in a measurement.

Fig 5. Poission Noise

3. ***Speckle Noise:-***

Speckle noise is a granular noise that inherently exists in and degrades the quality of the active radar and synthetic aperture radar (SAR) images. Speckle noise in conventional radar results from random fluctuations in the return signal from an object that is no bigger than a single image-processing element. It increases the mean grey level of a local area. The speckle can also represent some useful information, particularly when it is linked to the laser speckle and to the dynamic speckle phenomenon, where the changes of the speckle pattern, in time, can be a measurement of the surface's activity.

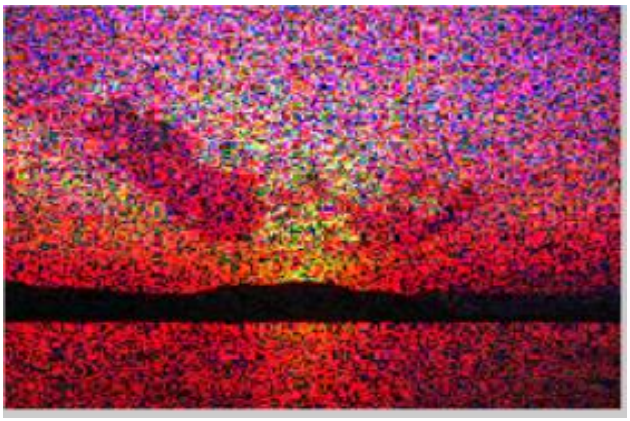

Fig 6. Speckle Noise

4. ***Gaussian Blur****:-*

A **Gaussian blur** (also known as Gaussian smoothing) is the result of blurring an image by a Gaussian function. It is a widely used effect in graphics software, typically to reduce image noise and reduce detail. The visual effect of this blurring technique is a smooth blur resembling that of viewing the image through a translucent screen.

Fig 7. Gaussian Blur

C. Peak Signal to Noise Ratio (PSNR):-

The PSNR value is used to evaluate the quality of watermarked image. The phrase peak signal to noise ratio (PSNR) is most commonly used as a measure of quality of reconstruction in image compression [9]. It is most easily defined via Mean Square Error (MSE) which for two m*n images I and J where one of the images is considered as a noisy approximation of the other (in other words, one is the original and the other is the watermarked image) [10]. Typical values for the PSNR are between 30dB and 40dB. If the PSNR of the watermarked image is more than 30, it is hard to be aware of the differences with the cover image by the human eyes system.

A. Reasons for Use of PSNR for evaluation of noise:-

- The PSNR is simple to evaluate.
- It is an expression for the ratio between the maximum possible values of the signal.
- The power of distorting noise that affects the quality of its representation.
- Signals have a very wide **dynamic range.**
- Ratio between the largest and smallest possible values of a changeable quantity.
- The **PSNR** is usually expressed in terms of the logarithmic decibel scale [11].

$$PSNR = 20 \log 10 \left(\frac{MAXf}{\sqrt{MSE}}\right)$$

With this formula we can calculate the PSNR value for each and every noise attacks ,so that we can compare which noise attack is efficient for encrypt the original image from hackers.

B. Mean Signal Error (MSE):-

The Mean Square Error (MSE*)* and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. This ratio is often used as a quality measurement between the original and a compressed image [4].The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower will be the error[5].

$$MSE = \frac{1}{mn} \sum_{0}^{m-1} \sum_{0}^{n-1} \|f(i,j) - g(i,j)\|^2$$

With this formula we can calculate the MSE value for each and every noise attacks, so that we can compare which noise attack is having the lower MSE value, the higher PSNR value and lower MSE value will give more distorted image for encryption.

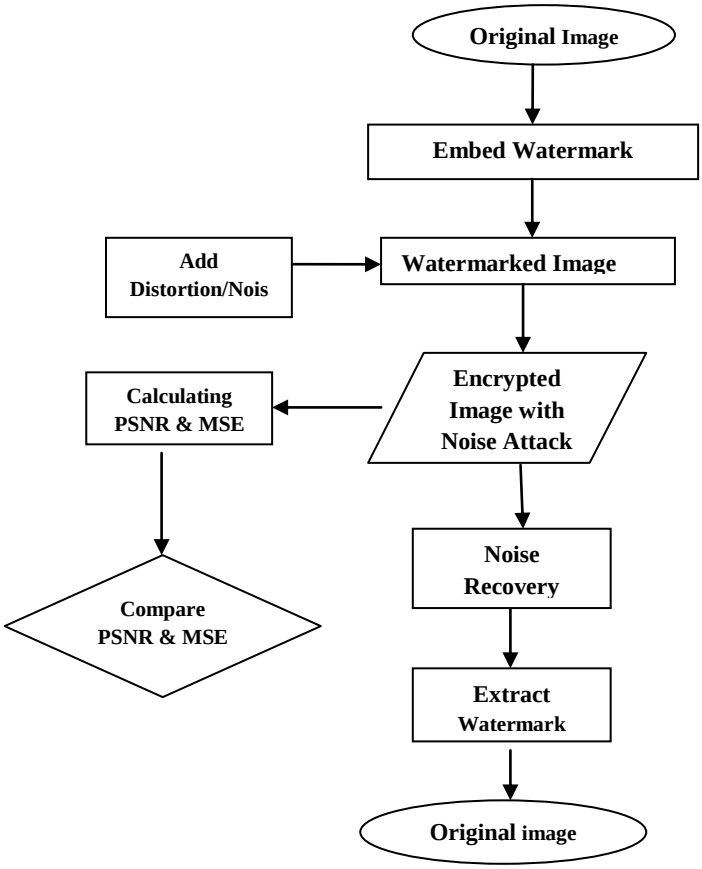

Fig 8. Flow Chart of Proposed Algorithm

IV. CONCLUSIONS

The proposed scheme is an efficient watermarking scheme that provides security for secured transmission of images requirements and evaluates LSB based image watermarking scheme with different noise attacks substitution After we have embedded the watermark in the image we got Watermarked Image without noticeable distortion on it. When we embed the different noise, the image start distorted. The PSNR and MSE values are calculated and higher value of PSNR image will give effective noise to images and the lower the value of MSE, the lower will be the error.

So our scheme is expected to serve as efficient and secure image. At the end of the proposed protocol has been provided some of the most important security criteria for the watermarking technique.

REFERENCES

[1] Puneet Kr Sharma1 and Rajni2, INFORMATION SECURITY THROUGH IMAGE WATERMARKING USING LEAST SIGNIFICANT BIT ALGORITHM,David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 61–67, 2012.

[2] R.AARTHI, V. JAGANYA, & S.POONKUNTRAN, Modified LSB Watermarking for Image Authentication, (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012.

[3] ABHISHEK ARVIND GULHANE, ABRAR SHAUKAT ALVI, Noise Reduction of an Image by using Function Approximation Techniques, (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[4] Deepshikha Chopra1, Preeti Gupta2, Gaur Sanjay B.C.3, Anil Gupta4, Lsb Based Digital Image Watermarking For Gray Scale Image, *IOSR Journal of Computer Engineering (IOSRJCE) (Sep-Oct. 2012).*

[5] Puneet Kr Sharma1 and Rajni2, ANALYSIS OF IMAGE WATERMARKING USING LEAST SIGNIFICANT BIT ALGORITHM, International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.

[6] Pawan Patidar ,Ashok Kumar Nagawat, Sumit Srivastava, Manoj Gupta Image De-noising by Various Filters for Different Noise,IJCA Nov 2010.

[7] Dr.M.Mohamed Sathik and S.S.Sujatha, An Improved Invisible Watermarking Technique for Image Authentication, Vol. 24, November 2010.

[8] P.RAMANA REDDY1, Munaga .V.N.K.PRASAD2, D. SREENIVASA RAO3, Robust Digital Watermarking of color images.(IJSER)2010.

[9] T.JAYAMALAR1, Dr. V. RADHA2, Survey on Digital Video Watermarking Techniques and Attacks on Watermarks, T.Jayamalar ,2010.

[10] AKSHYA KUMAR GUPTA and MEHUL S RAVAL,A robust and secure watermarking scheme basedon singular values replacement, Sadhan ¯ a¯ Vol. 37, Part 4, August 2012, pp. 425–440. c Indian Academy of Sciences.

[11] Mr. Rohith.S, Dr. K.N.hari bhat, A Simple Robust Digital Image Watermarking against Salt and Pepper Noise using Repetition Codes, ACEEE Int. J. on Signal & Image Processing, Vol. 03, No. 01, Jan 2012

About Authors Profile:-

Ms. Nidhi Bux received the B.E. From Pt. Ravishankar Shukla University, Raipur (C.G.), India in Computer Science & Engineering in the year 2008. She is currently pursuing M.Tech. Degree in Computer Science & Engineering with specialization in Computer Science & Engineering from CSVTU Bhilai (C.G.), India. She is currently working as Assistant Professor with the Department of Computer Science & Engineering in Garv institute of Management & Technology (GIMT), Durg, (C.G.) India. Her research areas include Cryptography, Computer Network & Pattern Recognition, and Image Processing etc.

Prof. Kashiram. Jayaram. Satao is Computer Science & Engineering and Head of Information Technology Department at Rungta College of Engineering & Technology, Bhilai (C.G.), India. He has obtained his M.S. degree in Software Systems from BITS, Pilani (Rajasthan), India in 1991. He has published over 40 Papers in various reputed National & International Journals, Conferences, and Seminars. He is Dean of Computer & Information Technology faculty in Chhattisgarh Swami Vivekanand Technical University, Bhilai, India (A State Government University). He is a member of the Executive Council and the Academic Council of the University. He is a member of CSI and ISTE. He has worked in various Engineering Colleges for over 25 Years and has over 4 Years industrial experience. His area of research includes Operating Systems, Editors & IDEs, Information System Design & Development, Software Engineering, Modeling & Simulation, Operations Research, etc.

