ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 9, September 2016

A Novel Spatial Domain Invisible Watermarking Technique Using Canny Edge Detector

[1]Vardaini

M.Tech, Department of Rayat Institute of Engineering and information Technology, Railmajra

[2]Anudeep Goraya
Associate Professor, Rayat Institute of Engineering and information Technology, Railmajra

***Abstract*— As the use of the internet is increasing rapidly the security has become the major concern for the user .Watermarking is one the method of process of sending the data securely to the destination form the source .The process of inserting of the watermark in the carrier signal is termed as the image watermarking. Various techniques for the image watermarking have been proposed till date. The techniques like DWT,DCT etc were used for the image watermarking process .In order to design an efficient image watermarking system, in which the quality of the watermark is not degraded and also the security of the system is increased a new technique is proposed for the watermarking process . In this paper the traditionally used frequency transformation is shifted to spatial transformation so that the internal properties of the image are preserved. An edge detection technique is used that will detect the edges of the image on which the data is to hide Along with this the key exchange algorithm is used that will improve the security of the process. From the results it is concluded that this method is efficient and better than the existing method of image watermarking.**

Keywords—Image watermarking; Key exchange algorithm; spatial domain techniques, Edge detection

I. INTRODUCTION

Image watermarking is termed as the process of hiding data in the the image. A watermark is embedded into the carrier signal. A carrier signal can be in the form of the text, video or image. The image watermarking is basically done on order to depict the identification of the owner to provide the copy right protection. Watermarking process is considered as the one of the reliable communication process transmitting the of the data from the source user to the destination user. Security is one of the major concerns while the data transmission takes place. All watermarking systems have, generically, two main steps: embedding of the watermark and the extraction of the watermark.

In the data insertion process the watermark is embedded in the carrier signal (also called as host signal) by this embedding process anew signal is obtained that is called as watermarked signal. For embedding of the data various data embedding techniques are used. In the data extraction process the data that is embedded earlier is extracted .watermarking process is used for wide number of applications

Some of the applications of watermarking are copyright protection, Tamper detection Validation of the Authentication and integrity, fingerprinting, Medical applications etc.

In this paper the technique for improving the security of the data is proposed. Also the edge detection technique is used that will help in the detection of the edges in which the data is to be hided in this way the data embedding method is also improved .

.

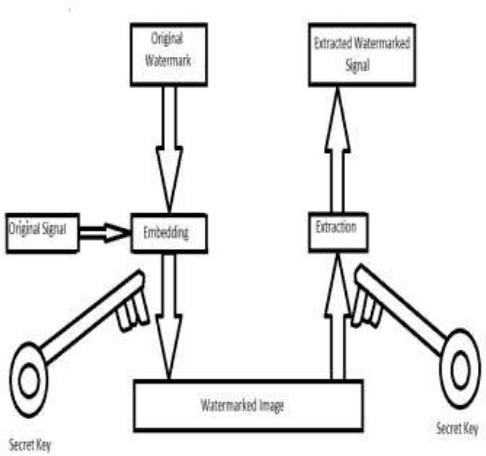

Figure 1: Block diagram of watermarking

II. PROBLEM OF TRADITIONAL APPROACHES

The process of inserting the watermark in the carrier signal in order to obtain an watermark signal is termed as the image watermarking process A watermark that is inserted can be in the form of the digital photo that can be a text or a copyright notice or a logo . The watermarking is used for identification of the copyright of the work so that it cannot be accessed by

any unauthorized user. Various techniques are used for embedding the watermark in the image so that the quality of the watermark is not degraded. If the watermark is degraded the process of watermarking will not be efficient. The watermark that is to be inserted should be robust against any sort of manipulation is done in the carrier signal as the watermark is inserted in the carrier signal. Security of the watermark is also a major issue of concern. The data that is to be hided should be done in the precise manner so that it is not visible to the unauthorized user. Various techniques have been proposed earlier but still the watermark systems are not that much secure.

III. PROPOSED WORK

Watermarking process is used for hiding the text or data into image. In case of visible watermark it is not possible to restrict the unauthorized access, it is more difficult for the one who claims the other data as their own . So in this proposed the problems arising the traditional technique are considered. By using DCT technique the image quality decreased so in this approach the frequency transformation is shifted to spatial transformation. The main advantage in moving spatial domain is that the internal properties of the image are not considered in this domain as it works on the front end features. So the edge detection technique is used that will detect the edges of the image on which the data is to hide. By using this the internal property of the image is not effected and the quality of the image is not degraded. In addition to this the key exchange algorithm is also used, before hiding the watermark into the image the key exchange algorithm is applied to increase the security of the watermark so that is not detectable .So this method is considered to be better and efficient than the traditional method of image watermarking as both the security and the quality of the image is increased. This work is proposed keeping following objective in mind.

1. To improve the security of watermarking technique
2. To improve the quality the image by proposed technique
3. By replacing the existing frequency domain technique with the spatial domain techniques
4. To use key exchange algorithm to increase the data security.

IV. EDGE DETECTION

It used for feature extraction and feature detection .In this edges of the digital image are marked, edge is defined as object border, and extracted by features such as gray, color or texture discontinuities ,the points at which image brightness change sharply are the edge. The purpose of detecting sharp changes in image brightness is to capture important events and changes in properties of the world. With the help of edge detection we can find the boundaries of the image. There are many methods of edge detection, but most of them are grouped in two categories, search based and zero crossing based. . The Edge contains important information of image and provides object's location. There are various methods of edge detection like Sobel, canny etc.

Some of the edge detectors have been described that are used for the detection of the edges of the images that are used for various purpose .

- Robert Edge detector
- Prewitt Edge detector
- Sobel edge detector
- Canny edge detector

Figure 2: Original image for edge detection

A. Robert Edge Detector

In this the derivate of the image is obtained at every pixel. This is the first detector that was designed for the edge detection process. It is implemented in two 2*2 masks. The partial derivates can be obtained by using equations given below :

$$G_x = z_9 - z_5$$
$$G_x = z_8 - z_6$$

These filter are efficient for the accurate detection of the position of the edges. The major disadvantage of this filter is that is more prone to the noise. Also the results are not better if the edges are not sharp .

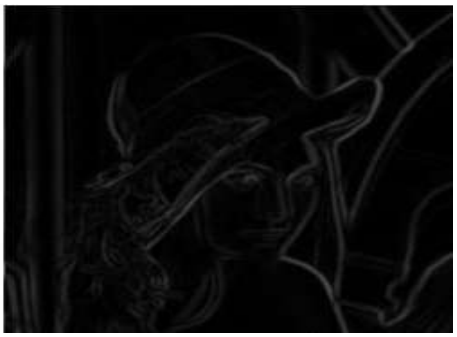

Figure 3: The edge detection using Robert detector

B. Prewitt Edge detector

This edge detector was designed to overcome the limitation of the Roberts's detector. This efficiently deals with the 3*3 masks having noise effect. The derivate of the perwitt edge dete3ctor is calculated by using the given equations

$$G_x = (z_7 + z_8 + z_9) - (z_1 + z_2 + z_3)$$
$$G_y = (z_3 + z_6 + z_9) - (z_1 + z_4 + z_7)$$

These detector are have longer support as compared with the Robert detector. These detector are less prone to noise the basic reason behind this is that they are differentiated in one direction and average in the other direction

Figure 4: The edge detection using Perwitt edge detector

C. Sobel edge detector

This is quite old method of edge detection. This detector was basically designed for performing the convolution in 2D spatial gradient. The convolution is performed between the two vectors that are based on the directions, after that it is used for working for the pixel gradient. This is a threshold that is used for the calculation of certain few coefficients. The coefficient calculated are defined as below :

$$G_x = (z_7 + 2z_8 + z_9) - (z_1 + 2z_2 + z_3)$$

$$G_y = (z_3 + 2z_6 + z_9) - (z_1 + 2z_4 + z_7)$$

Figure 5: The edge detection using Sobel detector

D. Canny edge detector

Canny edge detector is one of the efficient edge detectors that is used for the detection of the edges in the image. This detection operation of the edge detector is completed in the multi -stage that help in the detection of the wide range of edges in the image. It is used for wide range of application. These detectors are quite accurate as the error is quite less by using this detector. The detection of the edges is reliable process without any information loss.In this paper the Canny edge detector is used for the detection of the edges of the image in which the watermark is hided .

Figure 6: The edge detection using Canny detector

V. METHODOLOGY

In image watermarking the data is hided in the image, in the proposed work the firstly the edges are detected using the canny edge detector and then the data hiding technique is used for hiding the data in the original image .Along with this the Diffie Hellman key exchange is used for the secure transmission of the data . The proposed methodology consists of two parts one is encoding and other is decoded, the methodology of the work done is given below: -

A. Encryption Part

1) Initially an image is selected from the data se of te image in which data is to be embedded and is send to the reciever at other end.
2) After selecting the image , next step is to apply the edge detection algorithm on the selected image for the detection of the edge in which the data will be hided . the location of the edges detected are saved .
3) Now, Select an watermarked image from the given set of the watermarked images,
4) Now embed the watermarked in the edges detected of the original image. The embedding is done by using data embedding technique .
5) After embedding the data in the image , next step is to generate the Diffie Hellman key exchange and hide it into the image
6) Finally an Data embedded image is obtained by embedding the key into the image and is send to the receiver at the receiver end

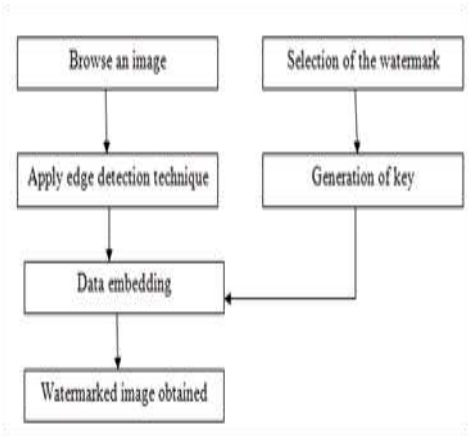

Figure 7: Embedding of the watermark in the image

Extration of watermark:
The watermark extraction is inverse of the watermark insertion process.

A. Diffie Hellman key algorithm

This protocol is considered as the one of the efficient cryptographic keys that will securely exchange the data over the communication link without any unauthorized access. It is also known as the exponential key exchange method. In this method the two parties can share a common message that can be used for generating a secret key that is used for the encryption process . It is the public key algorithm that will securely exchange the keys that encrypt data. The data is safe from the unauthorized access using this key algorithm.

VI. RESULTS AND DISCUSSION

In this section there is discussion about the results of proposed method of image watermarking. In this paper an approach is implemented for image watermarking. The following figures represent the processing of embedding and extracting the watermark. The edge detection process is used for the detection of the edges in the image in which data is hided.

A.

B.

C.

D.

E.

Figure 8: A. Original image B. Watermark image
C .Edge detected image D. Watermarked image
E. Extracted watermark

.

The following figure represents the results obtained by applying proposed method the following parameters are calculated. The parameters like BER, PSNR ,MSE are calculated

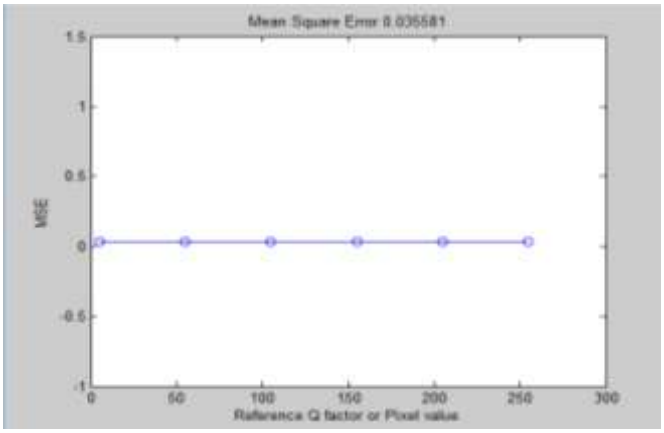

Figure 9: Graph depicts the MSE of the proposed work

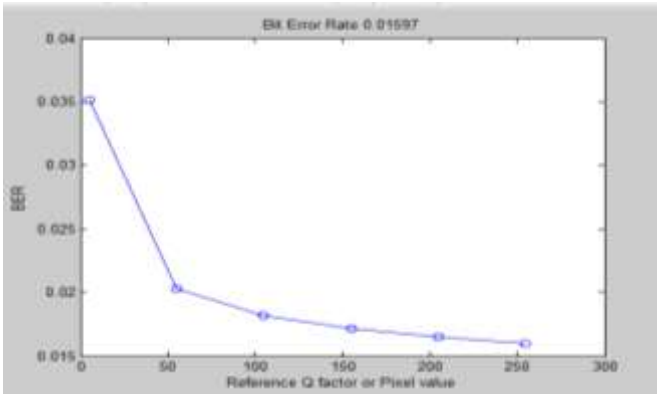

Figure 10: Graph depicts the BER of the proposed work

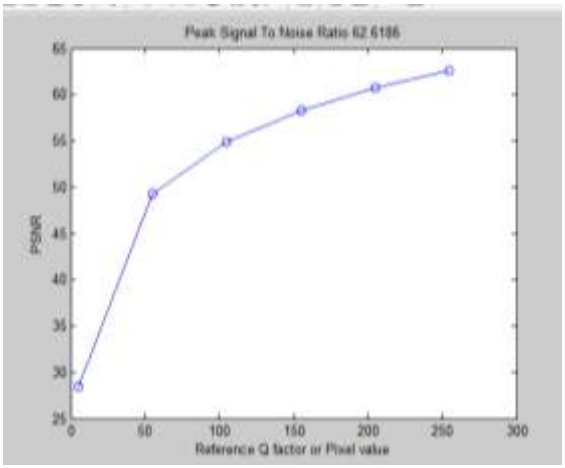

Figure 11: Graph depicts the PSNR of the proposed work

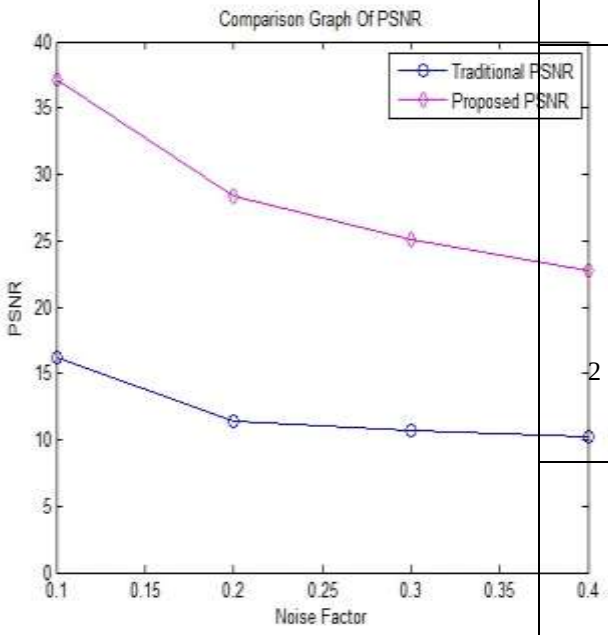

Figure 12 . The comparison between the proposed and the traditional approach on the basis of the PSNR

Table 1: The calculation of the PSNR proposed and traditional approach on the basis of the noise factor.(Lena picture)

S.NO.	Samples	Parameters Calculation
1		PSNR =62.8656 BER =0.015907 MSE =0.033614
2		PSNR =63.3182 BER =0.015793 MSE =0.030287
3		PSNR =62.6186 BER =0.01597 MSE =0.035581
4		PSNR =62.9775 BER =0.015879 MSE =0.0158792759

S.no	Noise factor	Old approach	Proposed approach
1	0.1	16.16	37.12
2	0.2	11.43	28.33
3	0.3	10.74	25.1186
4	0.4	10.23	22.78

Table 2: Represents the calculation of various parameters by using different images. The factors like PSNR, BER, MSE are calculated by using different images.

VII. CONCULSION AND FUTURE SCOPE

Watermarking is an efficient method of hiding the data in the carrier signal; this is done to increase the security of the data that is to send. Image watermarking is the procedure of hiding data in the images. From the results obtained it is concluded that this technique is better than the traditional techniques. In this proposed work the edge detection algorithm is applied for detection of the edges in which the data is hided .Along with this the key exchange algorithm is used that will increase the security of the watermarking method .From all parameters calculated it can be concluded that the performance of the proposed technique was better than the traditional technique. Also the security of the data is increased using this technique.

The proposed technique is better than the traditional techniques. It is analyzed that in future, further work can be done by using various other data hiding techniques or the hybrid approach can be used for hiding the data. Along with this various trending edge detection techniques can be used. Detection of edges in the image in which the data is hided. Also, the security of the watermarking can be increased.

REFERENCES

[1] Shankar Thawkar "Digital Image Watermarking for Copyright Protection" International Journal of Computer Science and Information Technologies, Vol. 3 (2) ,2012, Pp 3757-3760.

[2] Sunita "Review of Diffie–Hellman key Exchange "International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, 2013, Pp 285 -289 .

[3] Rohin "Enhancing the Diffie-Hellman Algorithm "International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 6,2014,Pp 448-452.

[4] Maryam Ahmed "Diffie-Hellman and Its Application in Security Protocols " International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, 2012, Pp 69 -73.

[5] Mr. Randhir Kumar "Analysis of Diffie Hellman Key Exchange Algorithm with Proposed Key Exchange Algorithm "International Journal of Emerging Trends & Technology in Computer Science Volume 4, Issue 1, 2015, Pp 40 – 43.

[6] J.R. Aparna "Image Watermarking Using Diffie Hellman Key Exchange Algorithm " ELSEVIER , Volume 46,2015, Pp 1684–1691.

[7] M.VidyaSagar "Modified Run Length Encoding Scheme for High Data Compression Rate" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 12,2013, Pp 3238- 3242.

[8] P. M.Sandeep "FPGA Bit-stream Compression Using Run-length Encoding"2013.

[9] J. Anitha "A Color Image Digital Watermarking Scheme Based on SOFM "IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5,2010, Pp 302-309.

[10] Jobenjit Singh Chahal " A Review on Digital Image Watermarking "International Journal of Emerging Technology and Advanced Engineering Website Journal, Volume 3, Issue 12, 2013,Pp 482 -484.

[11] Chandra, M. "Digital watermarking technique for protecting digital images" Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference ,Volume:7, 2010, Pp 226 – 233.

[12] Vinita Gupta M"A Review on Image Watermarking and Its Techniques" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1, 2014, Pp 92- 97.

[13] Manjit Thapa" Digital Image Watermarking Technique Based on Different Attacks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011, Pp 14 -19.

[14] Radhika v "Comparative Analysis of Watermarking in Digital Images Using DCT & DWT" International Journal of Scientific and Research Publications, Volume 3, Issue 2, 2013, Pp 1-4.

[15] Zhu Yuefeng"Digital image watermarking algorithms based on dual transform domain and self-recovery" international journal on smart sensing and intelligent systems vol. 8, no. 1, 2015, Pp 199- 219.

[16] M. Baritha Begum, December "A New Compression Scheme for Secure Transmission" International Journal of Automation and Computing 10(6), 2013, Pp 578-586.

[17] Amrita Jyoti, "An Advanced Comparison Approach with RLE for Image Compression" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, 2014, Pp 95- 99 .

[18] Neil F. Johnson "An Introduction to Watermark Recovery from Images".

[19] Amir Houmansadr "A Digital Image Watermarking Scheme Based on Visual Cryptography.

[20] Zhu Yuefeng "Digital image watermarking algorithms based on dual transform domain and self-recovery" international journal on smart sensing and intelligent systems vol. 8, no. 1, 2015, Pp 199- 219.