

Analysis of Watermarking in Digital Images by using Compression Technique

Payal Kaushal

M.Tech(CSE) student of
ASRA College of Engineering and Technology,
Bhawanigarh, Punjab, India

Navjot Kaur

Assistant Professor at
ASRA College of Engineering and Technology,
Bhawanigarh, Punjab, India

Abstract- With increasing use of internet the security of the data is the main concern. To secure data from the unauthorized access many techniques are used. Watermarking is one of such technique that is used for providing the security of the data. Digital watermarking is process of insertion of the watermark signal in the host signal. The digital watermarking system should be unappreciable, reliable and stable, etc. Earlier many watermarking techniques like DCT, DWT, and SVD were proposed for designing an efficient watermarking system. It was observed that the most of the work is done in embedding the watermark in the image but the security of watermark before it is embedded in the image is not considered anywhere. So in this a new method of image watermarking in which the security of the watermark is considered is proposed. The data compression techniques have been used to compress the watermark. Compressing the data will reduce the length and increases the security of the system. In addition to this a key exchange algorithm is also used that will provide additional security to the data.

Keywords—Image watermarking , Data compression, key exchange algorithm ,DWT, DCT,SVD

I. INTRODUCTION

Security plays an important role in the data communication. The data transfer should be reliable so that any unauthorized user is not able to access it. Watermarking can be considered as one of method that is user for reliable communication of the data. Watermarking is the process of hiding the watermark signal in the carrier signal. Carrier signal can be an image, video, audio etc and the watermarked signal can be in the form of image, text, video etc. Digital image watermarking is actually a derivative of Steganography, the ages-old practice of covertly transmitting a message from one party to other. All watermarking systems have, generically, two main steps: embedding of the watermark and the extraction of the watermark. In the embedding process the input are taken as the watermarked signal, carrier signal and a key that is used to embedded the watermark into the carrier signal , a new signal that is obtained is the watermarked signal. The reverse process, watermark extraction, is not the same for all watermarking systems. The extraction requires the watermarked signal. From which the watermark is extracted from the carrier signal. Robustness, perceptibility and capacity are the important factors that are taken in consideration while the watermarking system is designed. Watermarking is applicable for larger number of different applications like copyright protection, Tamper detection

Validation of the Authentication and integrity, fingerprinting, Medical applications etc.

Digital watermarking is an important branch of information hiding technology research field. With the development of the internet, watermarking technology for copy protection has great significance. Digital watermarking can indicate the copyright owner, identify the buyer or provide additional information of digital content, and embed the information into digital images, digital audio and video sequence.

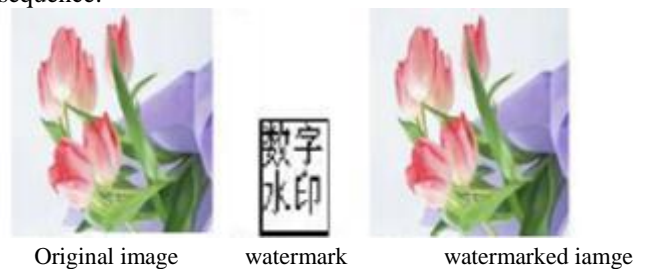


Fig 1 Watermarking process

II. TRADITIONAL TECHNIQUES OF IMAGE WATERMARKING

Watermarking is a technique used to hide data or identifying information within digital multimedia. Many methods of the watermarking have been proposed earlier, So that the data is securely transmitted without any unauthorized access. Some of the traditional techniques of the watermarking have been discussed below:-

- 1) Least significant bit (LSB) - it is the watermarking method that works in the spatial domain .In this method the least significant bit of the pixel is selected in which the information is directly inserted. The information is embedding is simple and effective. In this method no transformation is applied on the carrier signal during watermark embedding. The watermark can be detected by correlating the expected pattern with the received signal.

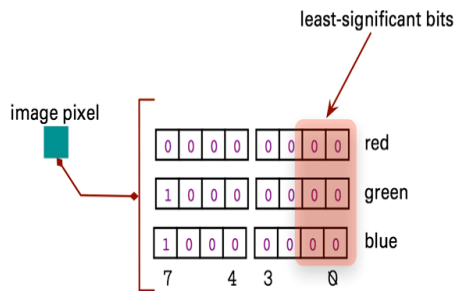


Fig 2 LSB concept of watermarking

2) *Discrete cosine transforms (DCT)* -it is one of popular frequency domain watermarking method. In this the carrier signal is divide into different frequency bands that are named as high, middle and low frequency band the information is inserted in the one of these bands. Mostly the middle band is preferred for the embedding of the information as the information do not get scatter in the middle band. In addition to this the watermark hided in the carrier signal is also not visible.

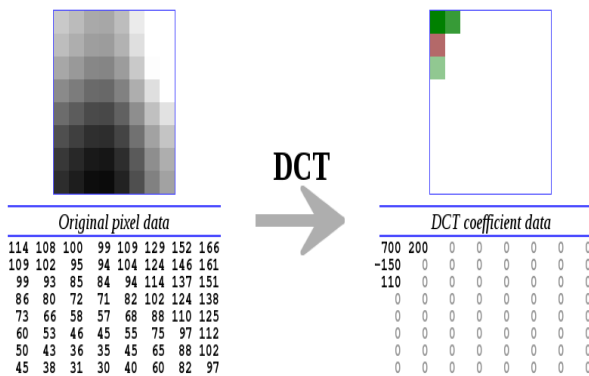


Fig 3. DCT concept of image watermarking.

3) *Discrete wavelet transform*: This is also a frequency domain watermarking technique. in this method the one dimensional signal is divided into two parts , one is the high frequency and other is the low frequency part . The edge components of the signal are present in the higher frequency part. The low frequency part is split into two parts and similar process will be continued till the desired level is achieved. In this each level the image is decomposed into the four parts. To do analysis e original signal DWT provides the sufficient information and requires less computation time. This watermarking technique will increase the robustness of the watermark

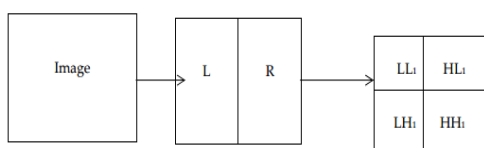


Fig 4. DWT decomposition process

4) Singular Value decomposition (SVD) :

The singular value decomposition (SVD) matrix is very useful in computer vision as a decomposition matrix and it is an efficient tool for image transformations. The SVD of a given image F in the form of a matrix is defined as:

$$F= USV^T$$

$$S = \begin{bmatrix} s_1 & 0 & \cdot & 0 & 0 \\ 0 & s_2 & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & s_{n-1} & 0 \\ 0 & 0 & \cdot & 0 & s_n \end{bmatrix}$$

And U and V are the orthogonal matrices = $UV^T=VU^T=I$
 $VV^T=I$

$$S_1, S_2, S_3 \dots S_{n-1}, S_n \geq 0$$

The diagonal elements of matrix S are the singular values of matrix F and non-negative numbers.

III. PROBLEM OF THE TRADITIONAL APPROACHES

Image watermarking is the process in which the watermark is inserted in the carrier signal in order to obtain the watermark signal. A watermark is a visible embedded overlay on a digital photo consisting of text, a logo, or a copyright notice. The purpose of a watermark is to identify the work and discourage its unauthorized use. In watermarking system if the watermark signal get distorted the watermark cannot be obtained back so to improve the quality of the signal, various technique are used for embedding the watermark. A watermark that is to be inserted should be robust against the modifications that can be applied to the carrier signal. So after studying these techniques it is was observed that the most of the work is done on embedding the watermark in the image but the security of watermark before it is embedded in the image is not considered anywhere. So the security of the embedded watermark is also an important factor that is to be considered while designing the watermarking system.

IV. PROPOSED WORK

In the proposed work, a new watermarking technique is introduced, in order to increase the security of the watermark that is to be embedded. In previous section the problem of the watermarking is defined. So to overcome that problem a data compression technique is used in this work. Using compression technique will reduce the length of the signal and will also increase the security of the data. The proposed method is considered to be better and efficient than the traditional methods for increasing the security of the watermark.

Data compression

Data compression is the processes of data that encode the data into small code without any loss of the information. By reducing the size of the dada the storage capacity increases, transmission time taken for sending the data over the internet will decrease, and the security of the data is also increases.

Advantage of the Data compression:-

- 1) When data is compressed, size of bits used to store information is reduced.
- 2) Transmission time of the data over internet is also reduced.
- 3) Security of the data is also increased.

Methodology of the proposed method

The methodology of the proposed work is divided into two sections, first part is the embedding the watermark and secondly extraction of the watermark:-

A) Embedding the watermark in the image

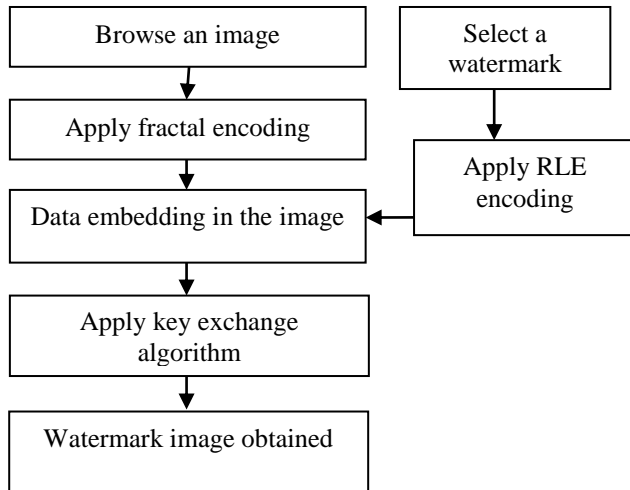


Fig 5 Embedding of watermark

For embedding of the watermark:-

- 1) Initially an image is browsed and the fractal encoding is applied on it.
- 2) Now, select a watermark image and apply RLE encoding for data compression
- 3) Embedded the watermark in the original image.
- 4) Apply the key exchange algorithm and generate a key.
- 5) A watermarked image is obtained.

EXTRACTION OF THE WATERMARK

The extraction of the watermark process is the inverse of the embedding process.

V. 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. We have use data compression technique before the watermarking is done

The following figures represent the processing of embedding and extracting the watermark



(A)

(B)



(C)



(D)

Fig. 6:- (A) Original image (B) Watermark image (C) Watermarked image (D) Extracted watermark.

The following figure represents the results obtained by applying proposed method the following parameters are calculated. The parameters like SSIM, PSNR are calculated. A comparison graph on the basis of the PSNR value obtained is calculated for traditional and the proposed approach

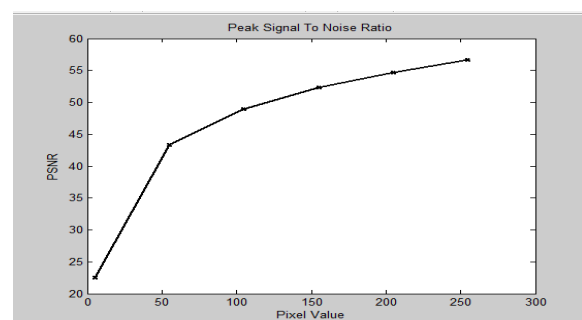


Fig 7 Calculation of PSNR

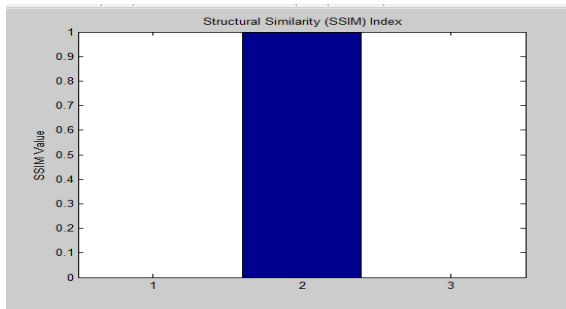


Fig 8 Calculation of SSIM

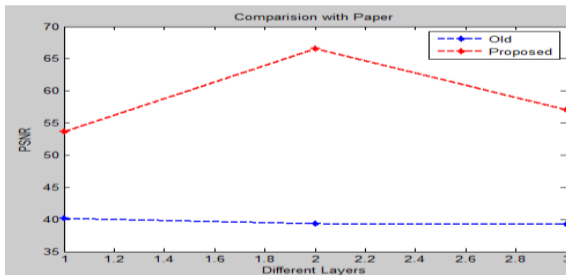


Fig 9 Comparison graph of PSNR

VI. CONCLUSION AND FUTURE SCOPE

It is observed after implementing the traditional methods of image watermarking they are not that much efficient in case of security issues, so in proposed work an approach of data compression and key exchange algorithm for increasing the security of the data is done. Performance parameters like PSNR, SSIM etc are calculated and compared on behalf of that it is concluded that proposed work is much efficient for image watermarking.

It is analyzed that in future further work can be done with videos. The media of the the data transfer is changed.

REFERENCES

- [1] Chandra, M.(2010), "Digital watermarking technique for protecting digital images" Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference , Volume:7, Pp 226 – 233,
- [2] Shraddha .S (2012), "Digital Watermarking: Review" International Journal of Engineering and Innovative Technology (IJEIT), Volume 1, Issue 2,Pp 143-153
- [3] Manjit Thapa (2011)" Digital Image Watermarking Technique Based on Different Attacks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4,Pp 14 -19
- [4] Radhika v(2013), "Comparative Analysis of Watermarking in Digital Images Using DCT & DWT" International Journal of Scientific and Research Publications, Volume 3, Issue 2,Pp 1-4
- [5] Zhu Yuefeng(2015), "Digital image watermarking algorithms based on dual transform domain and self-recovery" international journal on smart sensing and intelligent systems vol. 8, no. 1,pp 199- 219
- [6] Puneet Kr Sharma (2012), "Analysis of image watermarking using least significant bit algorithm "International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4,Pp 95 -101
- [7] Md. Selim Reza(2012), "An Approach of Digital Image Copyright Protection by Using Watermarking Technology" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2,Pp 280 -286
- [8] Shrusti Porwal(2013), "Data Compression Methodologies for Lossless Data and Comparison between Algorithms" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2,Pp 142- 147
- [9] Debashis Chakraborty, "Efficient Lossless Color Image Compression Using Run Length Encoding and Special Character Replacement"
- [10] M. Baritha Begum, December 2013, "A New Compression Scheme for Secure Transmission" International Journal of Automation and Computing 10(6), Pp 578-586
- [11] Amrita Jyoti, February 2014, "An Advanced Comparison Approach with RLE for Image Compression" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2,Pp 95- 99
- [12] M.VidyaSagar,(2013), "Modified Run Length Encoding Scheme for High Data Compression Rate" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 12,Pp 3238- 3242
- [13] P. M.Sandeep, March 2013, "FPGA Bit-stream Compression Using Run-length Encoding"
- [14] J. Anitha(2010), "A Color Image Digital Watermarking Scheme Based on SOFM "IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5,Pp 302-309
- [15] Jobenjit Singh Chahal (2013)" A Review on Digital Image Watermarking "International Journal of Emerging Technology and Advanced Engineering Website Journal, Volume 3, Issue 12,Pp 482 - 484