FEATURE POINT DETECTION USING K-HARRIES TECHNIQUE OVER SECURE IMAGE WATERMARKING

Gurwinder Kaur[1], Prof.Jaspreet Kaur[2]

[1]*Student, Instrumentation and control, BBSBEC Fatehgarh Sahib, Punjab, India,* **Rubybains26@yahoo.com**
[2]*Assist.prof.of Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib*

Abstract

This paper presents a digital image watermarking scheme using feature point detection and watermark template match. The digital image watermarking scheme, which is robust against a variety of common image processing attacks and geometric distortions. The image content is represented by important feature points obtained by our image-texture-based adaptive Harris detector. we take the original image and watermark image then we calculate the k- harries points (sharp points) on the original image. Now, the watermark image is resized because it is necessary that the watermark image is smaller than original image. Then the watermark image is divided into blocks in matrix. The watermark image is embedded into the original image. Then the harries points and image blocks extracted which gives the other watermark embedded image. The watermark image is compared with the embedded watermark image. To increase the embedding capacity the concept of watermark in watermark is used. To increase security we embed encrypted watermarks in the image. 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.

Index Terms: *Watermarking , K- Harries points detector , PSNR , Applications*

--- *** ---

1. INTRODUCTION

Because of the great advance and convenience in media technology, digitized information is being distributed widely and fast through network, such as Internet. The information carried by the watermark can be can be accessed using a detection algorithm provided the secret key is known. An important property of a watermark is its robustness with respect to image distortions. This means that the watermark should be readable from images that underwent common image processing operations, such as filtering, lossy compression, noise adding, histogram manipulation, and various geometrical transformations [1]. Watermarks designed for copyright protection, fingerprinting, or access control must also be embedded in a secure form. This means that an attacker who knows all details of the embedding algorithm except the secret key should not be able to disrupt the watermark beyond detection. There are three main watermarking techniques, audio watermarking, image watermarking and video watermarking, the most popular one of which is image watermarking, since image copyright protection is more urgent and is also the basic of video watermarking. Watermarking is a means of developing proper techniques for hiding proprietary information in the perceptual data [2].

2. IMAGE WATERMARKING

Digital watermarking is the process of computer-aided information hiding in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way, that it gets perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal. The image watermarking is applied for copyright protection, content authentication, detection of illegal duplication and alteration, feature tagging and secret communication. Digital watermarking is used in the hiding of a secret message or information within an ordinary message and its extraction at its destination. The secret message embedded as watermark can be almost anything, for example:

a serial number, plain text, image, etc. In general, digital watermarking involves two major operations:

(i) Watermark embedding

(ii) Watermark extraction.

For both operations a secret key is needed to secure the watermark .The keys in watermarking algorithms can be applied in the cryptographic mechanisms to provide more secure services to copy right protection [3].

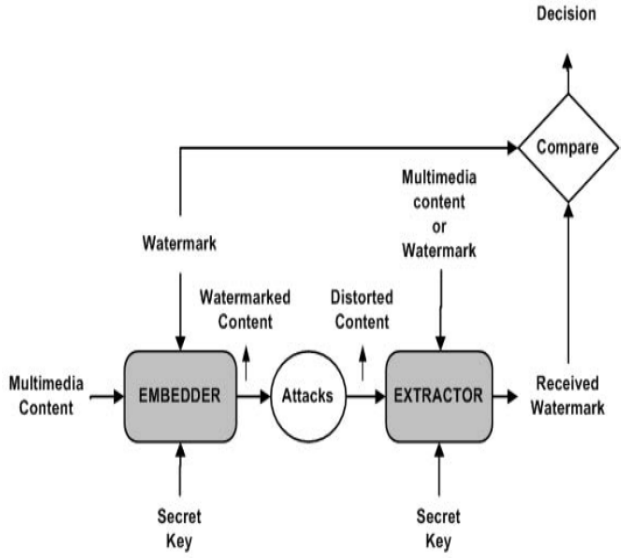

Fig-1: Watermarking System

2.1Watermark Embedding

For the embedding scheme, we chose to insert the watermark in the details (sub-images). In fact, the main interest of wavelet based techniques is that it ensures the imperceptibility's constraint and makes it possible. In addition, taking into consideration that the human visual system is not sensitive to small changes in high frequency that is, details, we proceed to insert watermark in these part of decomposed image. To ensure robustness, we used keys to embed and detect watermark. In the watermarking embedding system, the watermark image is divided into 3x3 blocks and the original image is calculate K-harries points. After that the watermark image blocks embedded one by one on the K-harries points of original image. Then the watermark image is embedded in original image.

2.2 Watermark Extraction

The extraction algorithm is straightforward and requires retrieving the original host image. The extractor need only compute the sum of the intensity values for the block of the host and watermarked image. A bit is decoded by making the comparison of the two resultant values. The watermark extraction system is used to extract the another watermark image from the original image. After that the embedded watermark image is compared with the extracted watermark image [4].

3. CLASSIFICATION OF WATERMARKING TECHNIQUES

Various types of watermarking techniques are enlisted below-

3.1. Inserted Media Category

Watermarking techniques can be categorized on the basis of whether they are used for Text, Image, Audio or Video.

3.2. Robustness

As a watermark is used to identify the owner of digital media, removal of the embedded watermark should be difficult for an attacker or any unauthorized user.

3.3. Public & Private Watermarking

In public watermarking, users of the content are authorized to detect the watermark while in private watermarking the users are not authorized to detect the watermark.

3.4. Inserting Watermark Type

Watermark can be inserted in the form of noise Tagged information, or Image.

3.5. Processing Method

We can classify the watermarking technique on the basis of whether we use spatial domain, frequency domain, compression domain or hybrid for the insertion of watermark.

4. K – HARRIES POINTS DETECTOR

This operator was developed by Chris Harris and Mike Stephens in 1988 as a processing step to build interpretations of a robot's environment based on image sequences. The Harris corner detector algorithm relies on a central principle: at a corner, the image intensity will change Largely in multiple directions [5]. This can alternatively be formulated by examining the changes of intensity due to shiftsin a local window. That is, for different distorted versions of the same scene, the detector should be able to extract similar, if not identical, points, despite variations due to a change of orientation or sharpness. The results of these studies prove the Harris detector is the most stable.

The second moment matrix *Ex,y* is defined by:

$E_{x,y} = (x,y)\ H\ (x,y)^{T}$ with $H = [\ D_{x,x}\, D_{x,y} : D_{x,y}\, D_{y,y}\ ]$

Ex,y can be considered as an auto-correlation function with a shape factor *H*. *D* represents image gradient of *x*- and *y*-axis. The corner-strength *RH* is acquired by combining the eigenvalues as follows.

$R_H = \mathrm{Det}(H) - k\mathrm{Tr}^{2}(M)$ where $\mathrm{Tr}(H) = D_{xx} + D_{yy}$,
$\mathrm{Det}(H) = D_{xx}\, D_{yy} - D^{2}_{xy}$

k is an arbitrary constant. Corner points are extracted by searching local maximums on this corner-strength of *RH*. This detector shows high accuracy in corner positions. However, the set of feature points is sensitive to image noise.

Fig-2: Original Image

Fig-3: Watermarking Image

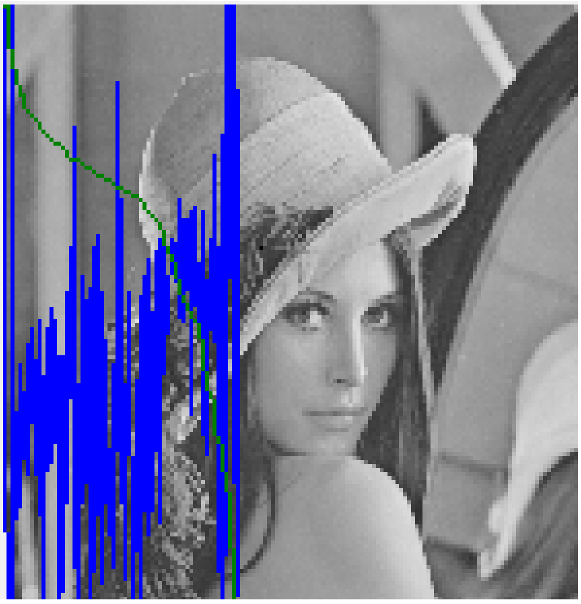

Fig-4: Calculated K-harries points in original image

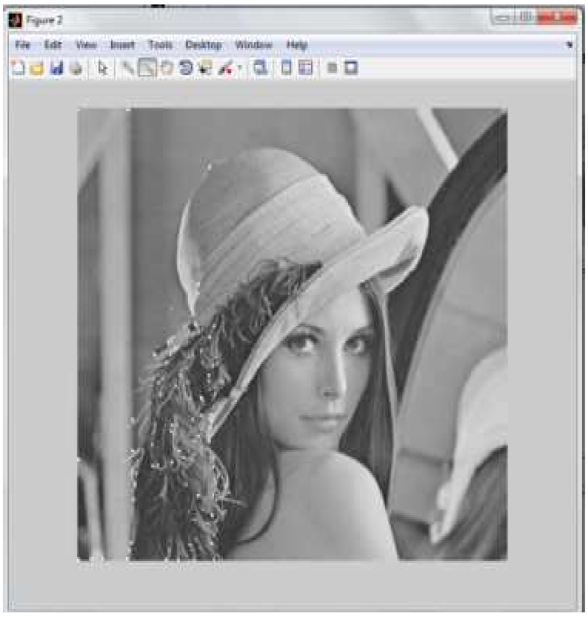

Fig-5: The Watermark image embedded into original image.

4. 1 Comparison Parameters

The images that have been regenerated after being compressed or after any other attack can be compared using BER, PSNR, and MSE. Any value of PSNR above 40 will be considered as the good value. This is related to maximum gray level value of any pixel so higher the better [6].

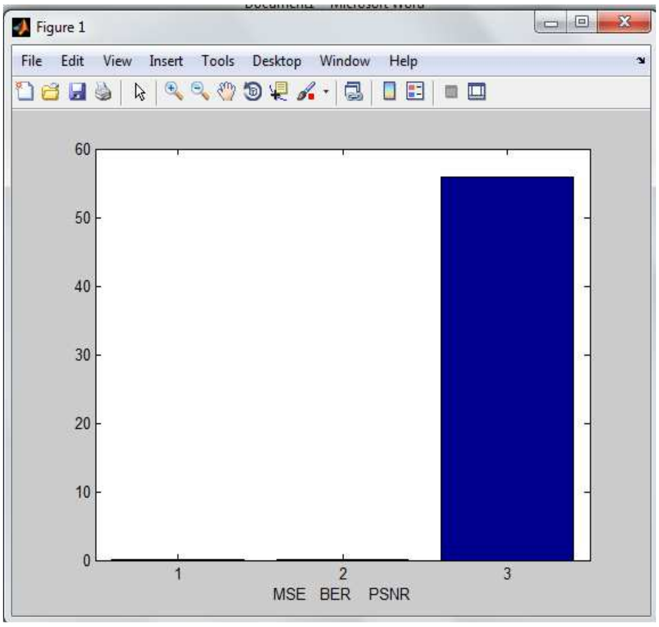

Fig. 6. Comparision b/w MSE , BER , and PSNR

5. APPLICATIONS OF WATERMARKING SYSTEMS.

5.1 Copyright Protection

The idea behind copyright protection is to embed information about the copyright owner into the data or cover image to prevent the third parties from claiming to be the authenticated owner.

5.2 Tracking

Digital watermarks can be used to track the usage of digital content. Each copy of digital content can be uniquely watermarked with metadata specifying the authorized users of the content. Such watermarks can be used to detect illegal replication of content by identifying the users who replicated the content illegally. The watermarking technique used for tracking is called as fingerprinting [7].

5.3 Tamper Proofing

Digital watermarks, which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content. The goal of this application is to detect alterations and modifications in a document [8].

5.4 Broadcast Monitoring

The system receives the broadcast and searches these watermarks identifying where and when the advertisement is broadcasted. The same process can also be used for video and sound clips.

5.5 Covert Communication

Covert communication is another possible application of digital watermarking. The watermark, secret message, can be embedded imperceptibly to the digital image or video to communicate information from the sender to the intended receiver while maintaining low probability of intercept by other unintended receivers [9].

5.6 Identity Card or Passport Security

Information in a passport or ID card can also be included in the person's photo that appears on the ID card. Extracting the embedded information and comparing it to the written text can verify the ID card. The inclusion of the watermark provides an additional level of security in this application. For example if ID card is stolen and the person replaces the picture, the failure in extracting the watermark will invalidate the ID card.

5.7 Medical Safety

Embedding the data and patient's name in medical image could increase the confidently of medical information as well as the security [10].

6. CONCLUSION

Watermark synchronization is crucial to design robust watermarking. One solution to find the location for watermark insertion and detection against image attacks is to use features. So, keeping in mind the security issues, it better to do it by embedding the watermark. By cascading the two watermarks one after the other, the robustness of the image increases as we try to compress the image the signal to noise ratio changes significantly. In which we use the K-harries points detector technique. Calculate the K-harries points of original image and the watermark image is embedded into the original image. After that the watermark image and the extracted watermark image compared on the basis of BER,PSNR and MSE. Other applications, such as fingerprinting, content authentication, copy protection and device controls have also been identified.

ACKNOWLEDGMENT

I am thankful to Dr. Gursewak Singh Brar (Associate Professor & Head of Department) who provided us with all amenities. We pay our regard for being given the much needed expert guidance. We also thank all my friends at college and teachers who provided us their much needed help.

REFERENCES

[1].Pratt, W.K.” Digital Image Processing” John Wiley & Sons, New York 1978

[2]. M.Rabbani and P.W. Jones, Digital Image Compression Techniques, Vol TT7, SPIE Optical Engineering Press, Bellvue, Washington (1991).

[3]. H. Inoue, A. Miyazaki, A. Yamamoto, T. Katsura, Digital watermark based on the wavelet transform and its robustness on image compression, in: Proc. IEEE Int. Conf. Image Process., vol. 2, 1998.

[4]. S. Pereira and T. Pun, “Robust template matching for affine resistant image watermarks,” IEEE Trans. Image Processing, vol. 9, pp. 1123–1129, June 2000.

[5] Arnold, M.; Schmucker, M; Wolthusen, S.D.; “Techniques and Applications of Digital Watermarking and Content Protection,” Artech House, 2003

[6]. C.-W. Tang, H.-M. Hang, A feature-based robust digital image watermarking scheme, IEEE Trans. Signal Process. 51 (4) (2003) 950–959.

[7]. T. Lindeberg, “Features detection with automatic scale selection,” Int.J. Comput. Vis., vol. 30, no. 2, pp. 79–116, 1998.

[8]. Zhang Deng-yin, Chen Jia-ping, Sun Jun-cai. Design and implementation of improved watermarking system in WT domain. The Journal of China Universities of Posts and Telecommunications,2007, 14(2): 58□63

[9].Podilchuk,C.I.;WenjunZeng;“Image-adaptivewatermarking using visual models,” IEEE Journal on Selected Areas in Communications, Volume: 16 Issue: 4, May 1998, Pages: 525

[10]. Mintzer, F.; Braudaway, G.; “If one watermark is good, are more better?,”Proceedings Int. Conf. Acoustics, Speech, Signal Processing, Volume 4, Phoenix,AZ, March 1999

BIOGRAPHIES

Gurwinder Kaur
I am doing Masters of Technology in Instrumentation and Control Engineering from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib.