ISSN:0975-9646

Ankita Sharma et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2399-2401

A Brief Introduction to Digital Watermarking

Ankita Sharma
M.Tech IV Sem.(CS),
GITS, Udaipur(Rajasthan)

Sarika khandelwal
Associate Professor,/ M.tech coordinator (CS dept.)
GITS, Udaipur (Rajasthan)

Abstract- From Last few year, internet became the first priority of everyone. It is a very easy and fast way to transfer and access data and information throughout the world. This information basically in the form of digital data (text, images, audio, video). Everyone using internet for their personal or professional use. Due to this it is important to protect user data from unauthorized access. When we talk about copy right protection means unauthorized person claim that copied data is created by him. What we do at that time? How can we prove that we are the right owner of data? to overcome this problem Digital watermarking mechanism is used in since to protect data from illegal copies or illegal distribution. It is a art of hiding information into digital data in a way , unauthorized person can't access or copy that data for misuse. Data which is insert into digital media is called watermark. It is a information (any label, citations, author name, id) about data. the proposed paper is an analysis of new enhancements in digital image watermarking techniques in both spatial domain and transform domain.

Key words- Transform domain, Digital image watermarking, DCT, DWT, DFT, SVD, spatial domain.

I INTRODUCTION

Due to enhancement of information technology distribution of digital data is become very easy. Increasing in development, increases security threads of data. It is important issue to protect multimedia data from many attacks such as counterfeiting, piracy and malicious maniple. To provide solution to many attacks number of mechanism used, digital watermarking is one of them.Watermark-It is a label, a tag, a information container which insert into multimedia data to make original data secure from illegal manipulation and distribution. It can be visible or invisible.

A) Digital image watermarking uses two type of watermark.

1) A. Pseudo-Random Gaussian Sequence: A Gaussian sequence watermark is a sequence of numbers contains 1 and -1 and which has equal number of 1's and -1's is denoted as a watermark. It is believe as a watermark with 0 mean and 1 variation. This type of watermarks are used for original data detection using a parallel measure.
2) Binary Image or Grey Scale Image Watermarks: watermarking algorithms insert information like logo image instead of a pseudo-random Gaussian sequence. This type of watermarks are considered as binary image watermarks or greyscale watermarks. Binary and greyscale watermarks are used for original data detection. Insertion of watermark depend on type of watermarking, To detect existent of watermark an appropriate decoder has to be used.

B) Watermark Properties:

1) Transparency or Fidelity: Quality of watermarked image should be remain same as original image. It should not affect the quality of the original image after it is watermarked. Watermarking should be distortions free because if such distortions are introduced it decreases the commercial value of the image.
2) Robustness: There are many image processing operations to remove watermark from original image. Such operations are contrast or brightness enhancement, gamma correction etc. watermark must have ability to bear such type of attacks.
3) Capacity or Data Payload: how much data should be embedded as a watermark to successfully detect during extraction. Capacity of watermark must be enough to represent data.
4) Imperceptibility: When invisible watermark is used for copy right protection and content authentication.It is necessary that watermark cannot be seen by human eye or not be heard by human ear, only be detected through special algorithm or circuit. It can be detected by an authorized agency only.

C) Types of Digital Watermarking

Digital Watermarking can be divided into various categories :

1) Based on object-

Text Watermarking: Watermark is embed into text file.
Image Watermarking : Watermark is embed into image.
Audio Watermarking : Watermark is embed into audio file.
Video Watermarking: Watermark is embed into video file.

2) Based on Human Perception-

Visible watermarking- Watermark is visible on objet.
Invisible watermarking- Watermark is not visible on objet.

Fragile-Watermark is invisible but affected by attacks means changes in watermark due to attack. Basically used in authentication The fragile watermark is very sensitive and designed to detect every possible change in marked image; so it fits to verify the integrity of data, and is viewed as an alternative verification solution to a standard digital signature scheme.

Semi-fragile-Watermark is invisible but Semi-fragile watermark fragile to malicious modifications while robust to incidental manipulations is drawing many attentions in image authentication.

Robust-Watermark is invisible but can bear communication attacks, means that watermark remain same as embedded.

II General Model Of Digital Image Watermarking:

The digital watermarking system essentially consists of a watermark Embedder and a watermark detector. By using watermark Embedder watermark is inserts onto the cover signal and using watermark detector detects the presence of watermark signal. An entity called watermark key is used during the process of embedding and detecting watermarks.

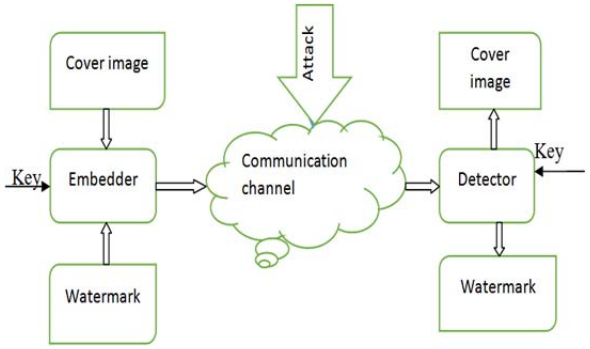

Fig-1 General Model of Digital Image Watermarking

III Units To Measure Capacity, Robustness And Quality Of Image Watermark

Determining the capacity of watermark in a digital image suggests that finding what quantity info is hidden in image while not perceptible distortion, whereas maintaining watermark strength against usual signal process manipulation and attacks. Knowing the watermark capability of a picture is beneficial to choose a watermark with a size close to the capacity or so as to enhance the strength, we are able to repeat embedding a smaller size watermark till reaching the capability. Typically capacity is expressed in bits per pixel (bpp) unit that is that the mean capacity of image pixels for watermark embedding. Image quality estimation measures like PSNR (Peak Signal to Noise Ratio), SSIM (Structural Similarity Index Measure), and JND (Just Noticeable Difference) square measure used for estimating quality degradation when watermark embedding. One among the foremost popular measures for watermark strength is Bit Error Rate (BER) that the amount of error bits in extracted watermark.

A)PSNR is most simply outlined via the mean square error (MSE). Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is outlined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR (in dB) is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

B) Structural Similarity (SSIM)- It is an index method for measuring the similarity between two images.

The SSIM metric is calculated on various images. The measure between two images x and y respectively of common size $N \times N$ is:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

here

- μ_x the average of x;
- μ_y the average of y;
- σ_x^2 the variance of x;
- σ_y^2 the variance of y;
- σ_{xy} the covariance of x and y;
- $c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$ two variables to stabilize the division with weak denominator;
- L the dynamic range of the pixel-values (typically this is $2^{\#bits\ per\ pixel} - 1$);
- $k_1 = 0.01$ and $k_2 = 0.03$ by default.

By using above formula's capacity and robustness of images can be calculated.

IV Research In Digital Image Watermarking

Min-Shiang Hwang'f, Chin-Chen Chang, present Watermarking Technique Based On One-Way Hash Functions in 1999 to provide secure watermarking system.

In 2000, Mohanty, S.P., Ramakrishnan, K.R., Kankanhalli, M.S.presnet a research paper on "A DCT Domain Visible Watermarking Technique for Images" in IEEE International Conference

In 2001, Yusuk Lim, Changsheng Xu and David Dagan Feng, present Web based Image Authentication Using Invisible Fragile Watermark"

Xiangui Kang, present a paper in IEEE conference "transactions on circuits and systems for video technology" in 2003 ,it present a digital watermarking using encryption.

In 2006, Harpuneet Kaur, R. S. Salaria, present a research paper on "Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data", in International Conference on Communication, Network, and Information Security (IASTED)

Bhupendra Ram Member IEEE present DWT AND DCT based digital image watermarking to provide robustness.

In 2012 Gupta introduced the concept of Cryptography based Digital image watermarking algorithm to increase security of watermark data by using the blind watermarking technique which uses watermark nesting and encryption. For encryption XOR operation was used and DWT based technique used for embedding watermark in cover image.

J S Bhalla and P Nagrath, had introduced the concept of Nested Digital Image Watermarking technique using blowfish algorithm. Here they mainly focused on increasing the embedding capacity and improving security of the watermarks by using LSB hiding technique for embedding.

In feb, 2014 , mayuri verma and Sheela verma present a research paper on "LSB HIDING USING RANDOM approach for image watermarking, in this paper Randomized LSB hiding algorithm is used for embedding one image into another as it has lesser complexity and the approach is more robust to the variations in the type of image. The blowfish algorithm is used to encrypt the watermark image before embedding into the cover image.

CONCLUSION:

This review paper provide a digital image watermarking brief introduction which provide us to get a instant knowledge about digital watermarking.

REFERANCES

[1] Min-Shiang Hwang'f', Chin-Chen Chang, **"**A watermarking technique based on one-way hash functions" ieee transactions on Consumer Electronics, Vol. 45, No. 2, MAY 1999

[2] Gurpreet Kaur and Kamaljeet Kaur, "Image watermarking using LSB " ,International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013

[3] Hebah H.O. Nasereddin, "Digital watermarking a technical overview" IJRRAS 6 (1) January 2011

[4] Saeed K. Amirgholipour , Ahmad R. Naghsh-Nilchi, "Robust Digital Image Watermarking Based on Joint DWT-DCT" International Journal of Digital Content Technology and its Applications Volume 3, Number 2, June 2009

[5] Seema Rana and Sheetal Sharma, "DWT-SVD Based Efficient Image Watermarking Algorithm to Achieve High Robustness and Perceptual Quality" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 10, October 2013

[6] Roshan Jahan," Efficient and Secure Digital Image Watermarking Scheme using DWT-SVD and Optimized Genetic Algorithm based Chaotic Encryption", International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013

[7] Bhupendra Ram Member IEEE, "Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013

[8] Pooja Dabas and Kavita Khanna, "Efficient Performance of Transform Domain Digital Image Watermarking Technique over Spatial Domain", International Journal of Engineering Research ,Volume No.2, Issue No.3, 2013

[9] Atul Barve and Veenita Gupta, "A Review on Image Watermarking and Its Techniques", International Journal of Advances in Science Engineering and TechnologyVolume- 1, Issue-3, Jan.-2014

[10] Aseem Saxena, "Digital Watermarking Using Matlab" , International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013 ISSN

[11] Kamaljeet Kaur, "Digital watermarking in spatial domain" Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013

[12] Prabhishek singh and R.S. Chad, "A Survey of Digital Watermarking Techniques, Applications and Attacks" International Journal of Computer Applications (0975 – 8887) Volume 4– No.8, August 2010

[13] Xiangui Kang, "Invisible Digital Watermarking Through Encryption" ieee transactions on circuits and systems for video technology, vol. 13, no. 8, august 2003

[14] Tuhin Utsab Paul, "DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression", International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010

[15] Mohanty, S.P.; Ramakrishnan, K.R., Kankanhalli, M.S.,"A DCT Domain Visible Watermarking Technique for Images." Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on , vol.2, no., pp.1029,1032 vol.2, 2000

[16] Dobsicek, M., Extended steganographic system. In: 8th Intl. Student Conf. on Electrical Engineering, FEE CTU 2004, Poster 04.

[17] Yusuk Lim, Changsheng Xu and David Dagan Feng, "Web based Image Authentication Using Invisible Fragile Watermark", Pan-Sydney Area Workshop on Visual Information Processing (VIP2001), Sydney, Australia, 2001

[18] Min Wu, Member, IEEE, and Bede Liu, Fellow, IEEE, "Data Hiding in Binary Image for Authentication and Annotation", IEEE Trans. Image Processing, volume 6, Issue 4, Aug. 2004

[19] Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, "Data Embedding Based on Better Use of Bits in Image Pixels", International Journal of Signal Processing Vol 2, No. 2, 2005