ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Review of Digital Watermarking Techniques

Tejaswita Salunkhe, Chhaya Nayak,

M. Tech Student, Dept. of CSE, B.M College of Technology, Indore, M.P. India

Assistant Professor& HOD, Dept. of CSE, B.M College of Technology, Indore, M.P. India

ABSTRACT: Digital image is the important vector of network information communication as there is rapid development of multimedia technology. In today's world, Security and reliability of images or information are the most important factors. During the transmission a process image often get destructed and fails to extract the hidden information as well as image authentication. In recent years, one of the widely used and developed techniques is digital watermarking. Digital watermarking is widely used in medical applications. There are several purposes of image watermarking. One of the widely used applications is to protect the patient's medical history from unauthorized people. It embeds the watermark like patient's information and doctor's signature in host's medical image for telemedicine applications. It can be also used for authentication if patient lost his/her image. This paper focuses on using wavelet transform in medical images watermarking. It discusses the wavelet transform watermarking technique. And it highlights the latest related work done on using wavelet transform watermarking over medical images.

KEYWORDS: Digital Watermarking, Wavelet transform, Medical Images

I. INTRODUCTION

Generally Watermarks are symbols which are added to the paper while manufacturing it for identification of manufacturer. First watermark were noticed in Italy during 13th century.[1]In recent years. Internet has become a very popular tool to transfer information. Information like text, sound, images and videos are transmitted through internet. That's why researchers have been facing many issues like confidentiality, reliability and availability. Digital watermarking is one of the proper solution to solve this issues. The basic idea of digital watermarking is to insert the information i.e. watermark into a host image. Then that watermarked image will be transmitted over the internet and at the receiver side information is extracted.

Digital watermarking technique is widely used in medical applications as CT scan and MRI has to be transmitted over the internet for proper diagnosis. Digital watermarking method is also used for the tamper proofing and authentication [2].Digital watermarking has wide range of applications including number of image processing techniques. The digital watermarking applications are Broadcast Monitoring [3], Digital Fingerprinting [4], Transaction Tracking [5], Copyright protection [6], Temper Detection [7], Data Hiding [8] and Content Authentication [9] etc**.**Many goals can be achieved by embedding the watermark into medical images. Three important goals are

1. If patient lost his/her medical image, then watermarked image authenticates the patient.
2. To protect the copyright and integrity of medical image watermarking is used.
3. To protect the patient's information from unauthorized people.

Patient's information, doctor diagnosis and Electronic Patient Records (EPR) can be embedded in the image as hidden watermarks. We can also add doctor's identification code in the medical images.

Types of Watermarks

The watermarking embedded into a media object is of two types that can either be perceptually visible or invisible.

1. Visible Watermark

A visible watermark is a visible translucent image that is overlaid on the primary image. It can be easily seen by human eye. Examples of Visible watermark are Name or company's logo or any copyright information .Visible watermark is used so that it can be read by receiver.[10]

2. Invisible Watermark

Human eyes are not able to detect invisible Watermark.The signal is not changed to great extent by invisiblewatermark.[11]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

II. DIGITAL IMAGE WATERMARKING WORKING

Digital Watermarking is a technique in which digital information is embedded into the multimedia data. Usually, this information is invisible, that is only dedicated detector can see and extract that information. In digital image watermarking digital image is used to embed the Information. It gives the watermarked image and it is more robust against attacks.[12]

Three stages of digital watermarking:

1. Embedding stage:
   In this stage watermark is inserted into the original image by embedding algorithm and secret key. It generates the watermarked image and it can be transfer over the network.
2. Distortion Stage:
   When the data is transmitted over the network either some noise is added with the watermarked image or some attacks are performed on the watermarked image. Watermarked data gets modified.
3. Detection Stage:
   By applying some detection algorithm the watermark is detected or extracted from the watermarked image.

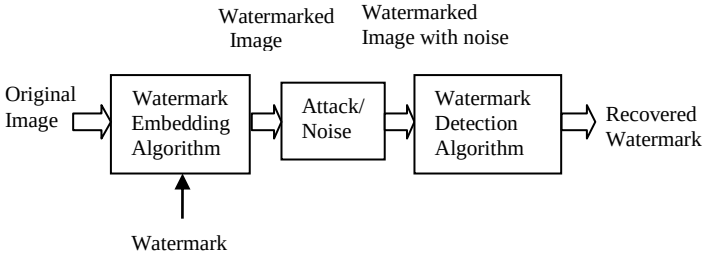

Figure: Stages in Digital Image Watermarking

III. DIFFERENT TECHNIQUES OF DIGITAL WATERMARKING

As we know, most of the world's information is stored in the form of readily transferable bits. So to provide authenticity to that data is becoming increasingly important.

Digital image watermarking has attracted a lot of awareness in the research community for two reasons: one is it convey enough redundant information and the other is its availability. Digital watermarking has various techniques for protecting the digital content. The digital watermarking technique mainly works in two domains either spatial domain or transform domain. In spatial domain technique, it directly works on pixels. Watermark is embedded by modifying the pixel values. LSB is the most commonly used technique in spatial domain. In transform domain, watermark is embedded by modifying the transform domain coefficients. DCT, DFT and DWT are the most commonly used transform domain techniques.[13]

In spatial domain image is represented in the form of pixels. Spatial domain technique modifies the intensity of pixels and their color value to embed the watermark.

Spatial domain watermarking strengths are:

1. Simplicity
2. Low computational complexity
3. Less time consuming

The computing speed of spatial domain is high as compare to the transform domain but it is less robust against attacks. This techniques can be easily applied to any image. The most important method of spatial domain is LSB.

A. Least Significant Bit (LSB)

LSB is the simplest spatial domain watermarking technique. It selects the some random pixels of the cover image to embed the watermark.[14]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Steps:

1. Conversion of RGB image to Gray scale image
2. Find double precision for image
3. Transfer most significant bits to low significant bits of watermarked image
4. Make least significant bits of host image zero.
5. Add shifted version (step 3) of watermarked image to modified (step 4) host image.

The important advantage of this method is that it is easily performed on images. It provides high perceptual transparency. When LSB technique is used to embed the watermark, quality of image will not degrade. Drawback of LSB technique is it is less robust to common signal processing operations. [15]

B. Discrete Wavelet Transform

In Discrete Wavelet Transform, it produces the multi resolution representation of an image. To interpret image information, multi resolution representation can be used as a simple framework. The DWT analyses the signal at multiple resolution. DWT divides the image into high frequency quadrants and low frequency quadrants. The low frequency quadrant is again split into two more parts of high and low frequencies and this process is repeated until the signal has been entirely decomposed.

The single DWT transformed two dimensional image into four parts: one part is the low frequency of the original image, the top right contains horizontal details of the image, the one bottom left contains vertical details of the original image, the bottom right contains high frequency of the original image. The low frequency coefficients are more robust to embed watermark because it contains more information of the original image [16]. The reconstruct of the original image from the decomposed image is performed by IDWT [17].

IV.REVERSIBLE WATERMARKING

In the last few years digital watermarking has grown explosively. It embeds an invisible/ visible watermark into digital content to protect and copyright communication. Digital watermarking methods are divided into two parts: robust watermarking and fragile watermarking. Robust watermarking is mainly used for copyright protection. Here robust means the embedded watermark should be resistant to various signal processing operations like scale, crop, compression etc. Fragile watermarking is used for content authentication. A fragile watermark can be altered or destroyed when the digital content is modified. Reversible watermarking has drawn lots of attention recently. Reversible watermark, (which is also called lossless watermark, invertible watermark, erasable watermark), has an additional advantage such that when watermarked content has been detected to be authentic, one can remove the watermark to retrieve the original, unwatermarked content. Such reversibility to get back unwatermarked content is highly desired in sensitive imagery, such as military data and medical data.

V.APPLICATIONS OF DIGITAL WATERMARKING

Digital watermarking is used in several applications.[19]The aim of every application is to providing security of the digital content. Following are the most important applications. [18]

1. Copy control.
2. .Digital copyright protection.
3. Transaction tracing and fingerprinting.
4. Broadcasting Synchronization System.
5. Digital content authentication and verification.
6. Forgery prevention.
7 .Lyric sync services.
8. Signatures.
9. Medical Application.
10. Fingerprinting.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

VI . WATERMARKING ATTACKS

Watermarking attacks are may be intentional or accidental. It is impossible to extract watermark by using intentional attacks as intentional attacks use all available resource to destroy or modify the watermark.[18] As every image processing or transmission noise may introduce distortions, the accidental attacks are inevitable.[20]Two more types of attacks are there as Estimation based attacks which estimates watermark using stochastic methods and estimation based attacks which are differentiated as follows:

1) Simple Attacks:

These attacks change the data of the cover image without attempting to target the watermark location. Example: Noise addition, cropping, conversion to analog and Wavelet-based compression.

2) Geometric Attacks:

Geometric attacks actually remove the watermark as well as manipulate the watermarked object so that viewer cannot find the watermarked data. These attacks occurred specifically on videos and images. Examples are rotation translation and scaling, warping, line removal, and cropping. But this process is very expensive and very complex.

3) Cryptographic Attacks:

These attacks are used for cracking the security. This attack works on security algorithm used for embedding watermark. For example, finding the secrete watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack [21].

4) Protocol Attack:

Most common example of protocol attack is deadlock attack. Deadlock attack is also known as fake-original attack, inversion attack or IBM attack[22]This attack embeds one or several additional watermarks such that it is unclear vwhich the watermark of the original owner was. Rewatermarking is the process of Watermarking of an already watermarked image. This type of attack can harm watermark application entirely.

5)Disabling Attacks:

To break the correlation between the watermark and the cover image, disabling attacks are used. Example: Geometric Distortions, rotation, cropping and insertion of pixels.

6) Ambiguity Attacks:

These attacks confuse the receptor by embedding a fake watermark, making it impossible to discover which the original embedded mark in the cover image was.

7) Removal Attacks:

In this type of attack a study of the watermark is carried out, estimating the watermark content and attempting to separate it from the host image.

Example:Certain non-linear filter operations and attacks tailored to aSpecific watermark algorithm. These attacks if it didn't success in the removal of the watermark completely; it destroys the watermark.

VII.CONCLUSION

Digital watermarking is very useful method for providing security to the digital media on the internet technology In this paper, we have reviewed Digital Watermarking technologies that hide information. In this paper we are briefly defining the concepts of watermarking, working of digital image watermarking, different techniques of digital watermarking, reversible watermarking, watermarking attacks as well as an applications. We are using data hiding by the simple LSB substitution method.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

REFERENCES

[1] Bing Ouyang Watermarking Based on Unified Pattern Recognition Framework UMI Number 3336693
[2] N. Tiwari, M. k. Ramaiya and Monika Sharma, "Digital watermarking using DWT and DES", IEEE 2013
[3] L. Li and X. Li," Watermarking Protocol for Broadcast Monitoring", International Conference on E business and E-Government (ICEE) (2010).
[4] D. Zhang, S. Xu, Y. Wang, J. Zhang and Y. Li, "A Digital Fingerprinting Scheme of Digital Image". International Conference on Computational Intelligence and Software Engineerin (CISE) (2010).
[5] S. Emmanuel, A. P. Vinod, D. Rajan and C.K. Heng, "An Authentication Watermarking Scheme with Transaction Tracking Enabled", Digital Ecosystem and Technologies Conference, 2007.DEST'07 Inaugural IEEE-IES.
[6] Y.-C. Wang and J.-f. Niu, "Research on Digital Content Copyright Protection System", IEEE International Conference on Network Infrastructure and Digital Content, 2009. IC-NIDC (2009).
[7] S.-L. Hsieh, C.-P. Yeh and I-J. Tsai, "An Image Copyright Protection Scheme with Tamper Detection Capability", Symposia and Workshops on Ubiquitous, Autonomic and trusted Computing,2009.UIC-ATC'09
[8] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication", IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 4.
[9] J. Zhu, Q. Wei, J. Xiao and Y. Wang," A Fragile Software Watermarking Algorithm for Content Authentication", IEEE Youth Conference on Information, Computing and Telecommunication, 2009.YC-ICT'09.
[10] Kutter M. and Petitcolas F. A. P. ,"A fair benchmark for image watermarking systems",(1999) In Proceedings of the SPIE Security and Watermarking of Multimedia Contents, vol 3657, pp 226 – 239
[11] Mohanty S. P., Ramakrishnan K. R., and Kankanhalli M., (1999) "A dual watermarking technique for images", In Proceedings of the 7th ACM International Multimedia Conference, ACM-MM'99, pp 49- 51
[12] L. Robert and T. Shanmugapriya," A Study on Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, vol. 1, no. 2, (2009) May.
[13] M. Hamad Hassan, and A.A.M.Gilani, "A Fragile Watermarking Scheme for Color Image Authentication", International Journal of Applied Science, Engineering and Technology, Vol. 1, No. 3, pp.-156-160, 2005.
[14] N. Pantuwong and N. Chotikakamthorn, "Line watermark embedding method for affine transformed images", ISSPA 2007, PP. 1-4, 2007.
[15] S. Riaz, M. Y. Javel, and M. A. Anjum, "Invisible watermarking scheme in spatial and frequency domains", International Conference on Emerging Technologies, 2008.
[16] N. Tiwari, M. k. Ramaiya and Monika Sharma, "Digital watermarking using DWT and DES", IEEE (2013).
[17] S. S. Gonge and J. W. Bakal, "Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum", International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, vol. 1, no. 2, (2013).
[18] J.Liu and X.He, "A review study on digital watermarking", 1st International Conference on Information and Communication Technologies, pp. 337-341, 2005.
[19] Edin Muharemagic and Borko Furht "A survey of watermarking techniques and applications" 2001.
[20] Friedman, G.L., "The Trustworthy Digital Camera: Restoring Credibilityto the Photographic Image", IEEE Transaction on Consumer Electronics, Vol. 39, No. 4, November 1993, pp. 905-910.
[21] G. Coatrieux, L. Lecornu, Member, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member IEEE, "a review of digital image watermarking healthcare".
[22] F. Hartung, J.K. Su., and B.Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks", pp. 147-158, 1999.
[23] Hebah H.O. Nasereddin ,"DIGITAL WATERMARKING A TECHNOLOGY OVERVIEW" IJRRAS January 2011
[24] Yusuf Perwej, Firoj Parwej , Asif Perwej, "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection" The International Journal of Multimedia & Its Applications (IJMA) Vol.4, No.2, April 2012
[25] Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh, "A Review of Different Techniques on Digital Image Watermarking Scheme" International Journal of Engineering Research (ISSN : 2319-6890) Volume No.2, Issue No.3, pp : 193-199
[26] Preeti Parashar, Rajeev Kumar Singh, " A Survey: Digital Image Watermarking Techniques" International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014), pp. 111-124

BIOGRAPHY

Tejaswita Rajendra Salunkhe is M.Tech student in Department of Computer Science Engineering, B.M. College of Technology , Rajiv Gandhi Technical University. She received Bachelor of Computer Engineering degree in 2010 from NMU, Jalgaon , MS, India.