www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 6 June 2017, Page No. 21708-21712
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i6.25

Survey on Digital Image Watermarking & Techniques

Yogesh Kumari
Assistant Professor, Department of Computer Science
Shivaji College, Delhi University, New Delhi, INDIA
Email id: yogeshkumari.cs.du.2013@gmail.com

Abstract:

In the past few decades Internet and digital technology has grown rapidly. The increasing and rapid advancement of Internet has made it extremely easy to send multimedia data accurate and fast to destination. It has provided various advantages like easy sharing of digital images, copying of digital images without quality degradation and editing of digital images. Also due to increasing trend of Internet, multimedia data is tend to duplicate and modify which makes multimedia security as an extreme concern to take care of. Modification and misusing of valuable data is very common and thus sending multimedia data to intended recipient has become more important. The problems arises includes privacy, corruption or processing of image and counterfeiting. This paper throws light on information hiding in order to protect original data from illegal duplication, distribution and manipulation through ”Digital Image Watermarking”. Watermarking is an art of hiding information into another file, which could be video, audio, text or image. The paper includes various type of watermarking, different techniques of watermarking.

Keywords- Digital Image watermarking, classification of watermarking, robustness, watermarking techniques

1. INTRODUCTION

With the increasing use of Internet, challenges to protect digital data from privacy has become a serious concern. Digital watermarking provides a robust solution to this security concern. For the protection of ownership rights of digital images, Digital image watermarking is one of the most widely used technique today. Digital image watermarking is the potential solution of content authentication, protection of images, copyright management, temper detection and protecting ownership rights against any unauthorized copying or redistribution of images. In digital image watermarking, secret information is embedded in digital media that you want to deliver to a particular recipient. The secret information called watermark that can be a binary bit sequence or text or an image which can be used to prove the right owner of the information shared. This may be used to verify authenticity and identity of the owner.

Watermarking Life Cycle Phases

The secret information embedded in digital media is called digital watermark. The watermark embedded in digital media is called host signal.[1] Host signal is basically the data in which watermarking is to be done. The host signal can be image, video, text or audio. The watermarking system is usually divided into three steps

I. Embedding Process (insertion)
II. Attack
III. Extraction Process (detection)

In embedded process, the algorithm takes the source image and information to be hide and sometimes require key and produces a watermarked image/signal.

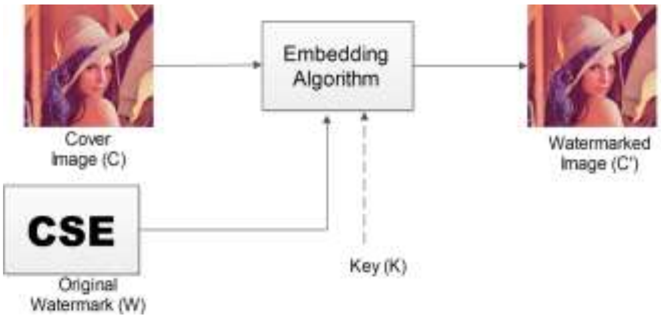

Figure1: Digital Image Watermarking Embedding Process

The input is watermark that is the secret information which can be used to authenticate or identify the legal owner, cover image that is the information to be transferred to desired recipient or key which is optional. The output produced is watermarked image that is transmitted to desired recipient.

If somewhere anyone tries to modify or alter the watermarked image, is called as attack. It may possible that modification made is not malicious but it will distort the quality of image. The various attack includes adding noise intentionally, cropping, duplication or compression of data. [2]

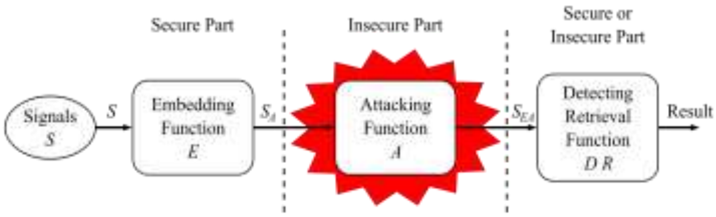

Figure2: general Digital watermarking life cycle phrases including embedding, attacking and detection and retrieval function

In extraction process, the algorithm is used to extract the embedded watermark from the watermark image so that it can be used to authenticate the identity of legal owner.

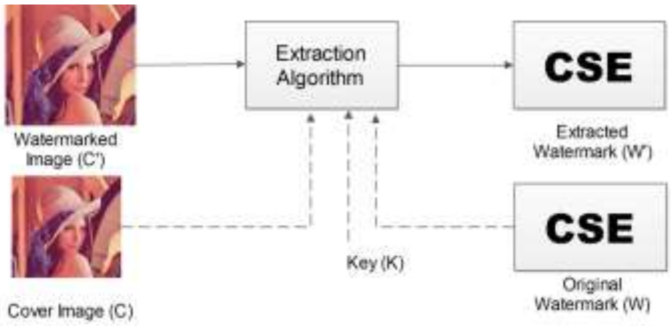

Figure 3: Digital Image Watermarking Extraction Process

The input is watermarked images, cover image, original watermark or security key if applicable. The produced output is recovered watermark or any confidence measure indicating probability of presence of watermark in the watermarked image.

2. Requirements of Digital Image Watermarking

When it comes to digital image watermarking some design features must be taken into consideration. Some important features of digital image watermarking are as follows

1 .Robustness
Robustness is one of the major design issues in terms of digital image watermarking. The digital watermark image must not be removed from the watermarked image when it placed onto different types of attack. [7] The digital watermark should be robust against compression and geometric transformation of host image, linear or non-linear filtering of host image, signal processing attack like D/A or A/D conversion. The embedded algorithm is tends to be good if it provides the maximum robustness. The maximum robustness of digital watermark means maximum attacks would be avoided.

2. Imperceptibility
The watermark can neither be seen by human eyes nor heard by human ear. The watermark is said to be imperceptible if the original image or watermark image are perceptually distinguishable. The watermark can only be detected through special processing or any dedicated circuits.

3. Data Payload
Data payload is the maximum amount of information that can be embedded in any image without degrading its quality. Data payload is the number of watermark that one can embedded within host signal. With host signal, audio, data payload is basically the number of watermark bits, measured bits per second (bps). Data payload or capacity of watermarking is determined by the statistical model used for host signal, distortion constraints on data hider and the attacker.

4. Security
The watermark owns the unique information to identify only the authorized user who can extract or modify the watermark and also achieve purpose of copyright protection. The watermark should survive deliberate attempts when it comes to removing it.

In digital image watermarking, effect of one requirement may affect another requirement. For instance, increased robustness tends to decrease the imperceptibility. Hence, there is a need to balance the trade-off between all the characteristics of digital watermarking according to the need or requirement of application.

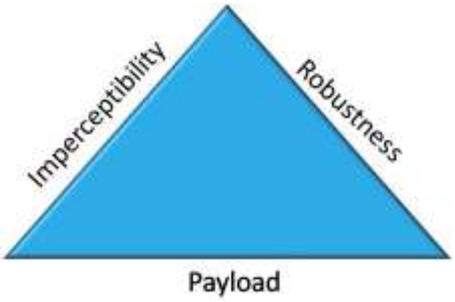

Figure 4: Requirement trade-off of digital image watermarking

3. Classification of Watermark

3.1 Based on Perceptibility

3.1.1 Visible watermark
The visible watermark can be seen by HVS, like stamp on a paper. For instance, channel logo is visibly superimposed to show watermarked image.

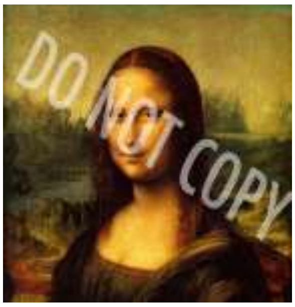

Figure 5: Visible watermark

3.1.2 Invisible watermark
Watermark is embedded in such a way that it cannot be seen by HVS but can be interrogated through any special software. Original image and watermarked image seems to be similar.

Figure 6: Invisible watermark

3.2 Based on Detection Process

3.2.1 Blind watermark

Blind watermarking doesn’t require original data at the time of detection of hidden information. These are less robust to any attacks.

3.2.2 Semi blind watermark

Semi blind watermarking require special information to detect the embedded information in the watermarked signal. [2]

3.2.3 Non-blind watermark

Non-blind watermarking requires the original image in order to detect the watermark in the watermarked image. It is more robust to attacks as compared to blind watermarks.

3.3 Based on Robustness

3.3.1 Robust watermark

A digital watermark is said to be robust when it resists benign transformation. Robust watermarking is used in copy protection and control.

3.3.2 Fragile watermark

When the digital watermark becomes undetectable even with the slightest modification made on watermarked image, is said to be fragile watermark.

3.3.3 Semi-fragile watermark

Semi-fragile watermark is capable of tolerating some degree of transformation to watermarked image.

4. Applications of Digital Image Watermarking

Digital image watermarking may be used in wide variety of applications.

1. Broadcast monitoring

Since over the past few years, the number of television and media vehicles delivering content has expanded notably. And it continues to increase exponentially. So, how does content owners manage their media assets and ensure fair compensation?

The embedding of digital watermark in audio or video or image content at the time of broadcast or production keep track of broadcast content. When and where the content is broadcast, who is broadcasting and for how long the content was broadcast. The digital image watermarking is serves as the broadcast management tool which provides valuable information of producers, content owners and broadcasters.

The following services are provided through digital Image watermarking:

(i) Identify potential misappropriation of assets
(ii) Evaluate true reach of media assets
(iii) Confirm and prove content broadcast and usage
(iv) Electronically verify invoices
(v) Verify contracts and invoices for ultimate accuracy and accountability

Figure 7: Advertisement

Figure 8: Broadcasting

2. Temper Detection

Temper detection is important when there is any modification or alteration made to original image. Temper detection is important for applications that involves highly sensitive information.

For instance, the number plate of car has been tempered to save from police case which is detected by digital image watermarking.

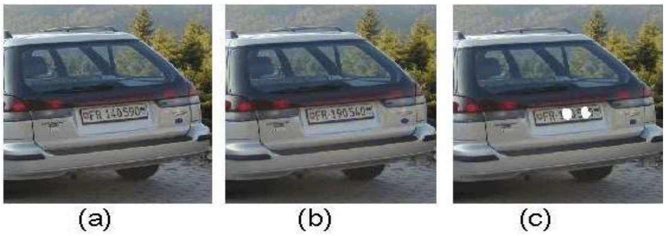

Figure 9: Temper Detection

3. Fingerprinting

The digital watermarking is used in applications where media content is distributed over a network. The content owner discourage unauthorized duplication and distribution of data by embedding a watermark or say, fingerprint in each copy of data. If later, any authorized copy is found, origin of copy can be determined by retrieving the fingerprint. In fingerprinting, watermark needs to be invisible and invulnerable to forge, remove or invalidate.

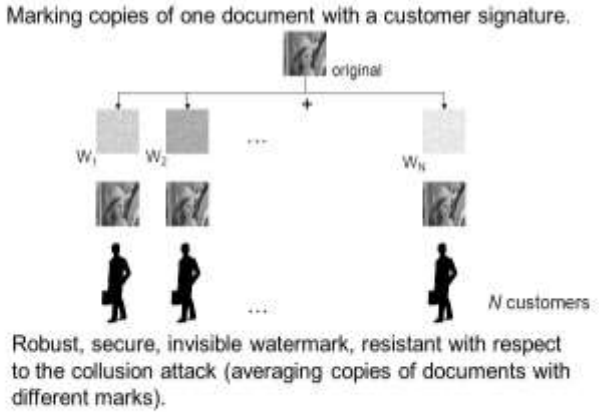
Marking copies of one document with a customer signature.
original
W1
W2
...
WN
...
N customers
Robust, secure, invisible watermark, resistant with respect to the collusion attack (averaging copies of documents with different marks).

Figure 10: Fingerprinting

4. Copy control

Watermarking is used for copy control and prevention. Digital watermarking is used to prevent illegal copying of copyright content. For instance, when media content requires special hardware for copying or viewing the content, digital watermark can be inserted representing the number of copies permitted. Each time a new copy is made, watermark is modified by hardware and after a particular limit, and it will not create any further copies of data.

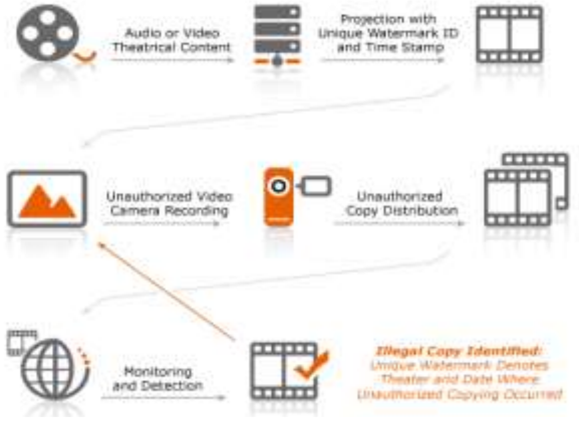
Audio or Video Theatrical Content
Projection with Unique Watermark ID and Time Stamp
Unauthorized Video Camera Recording
Unauthorized Copy Distribution
Monitoring and Detection
Illegal Copy Identified: Unique Watermark Denotes Theater and Date Where Unauthorized Copying Occurred

Figure 11: Copy control

5. Digital Image Watermarking Techniques

Digital image watermarking techniques can be broadly classified into two major sections:

5.1 Spatial Domain Watermarking

In Spatial Domain watermarking technique, watermark is embedded by modifying pixel intensity value of cover image. This technique is not reliable when subjected to operations like lossy compression or filtering. Various spatial domain techniques are as follows:

5.1.1 Least Significant bit coding (LSB)

Least significant bit coding is one of the earliest method that can be applied in any form of watermarking. The sequence of watermark bits are embedded by substituting the least significant bit of the carrier signal or cover image. LSB watermarking technique is vulnerable to attacks and watermark can be easily destroyed. The technique is highly sensitive to noise and common signal processing.

5.1.2 Predictive Coding Schemes

Predictive Coding schemes, the correlation between the adjacent pixels are exploited. The set of pixels where the watermark need to embed is chosen and alternate pixels are substituted by the difference between adjacent pixels. Predictive Coding Schemes is more robust as compared to LSB coding.

5.2 Frequency Domain

In frequency domain watermarking technique, watermark is embed by modifying frequency coefficient using various transforms. [2] Some of the most commonly used frequency domain are as follows:

5.2.1 Discrete Fourier transform (DFT)

Discrete Fourier transform performs an operation that transforms a continuous function into its frequency components. DFT of an image provides a quantitative picture of frequency in term of magnitude and phrase. The image produced is robust to rotation, scaling and transformation variant. But the only disadvantage of output produced by DFT is its complex value. [2]

5.2.2 Discrete Cosine Transform (DCT)

Discrete Cosine Transformation transforms a signal from spatial domain to frequency domain. This technique may be applied in many fields including data compression, pattern recognition and image processing. But the only disadvantage is that DCT is weak against geometric attacks which includes rotation, cropping, scaling and more.

5.2.3 Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform is one of the modern techniques used in digital image processing, compression and watermarking. The technique is based on small waves of varying frequency known as wavelets. DWT models HVS more accurately as compared to other transforms, DFT and DCT. DWT allows higher energy watermark in regions where HVS is less sensitive, as a result, it increases robustness of watermark and thus no degradation of image quality.

6. CONCLUSION

The purpose of this paper is to present a survey of digital image watermarking and its techniques. Various type of watermark, techniques and real-life applications have been analyzed in this paper. When it comes to working domain of watermarking techniques, transform or frequency domain provides more robustness, better results of bit rate error as compared to spatial domain watermarking technique. In near future, watermark would be so efficient to tell any image where it is originated, date distributed and to whom it was distributed.

REFERENCES

[1] Chauhan Usha , Singh Rajeev Kumar, Digital Image Watermarking Techniques and Applications: A Survey", India March 2016

[2] Shraddha S. Katariya, "Digital Watermarking: Review", International Journal of Engineering and Innovative Technology, ISSN:2277-3754, Volume 1, Issue 2, February 2012.

[3] Prof. Manoj Ramaiya Richa Mishra, " Digital Security using Watermarking Techniques via Discrete Wavelet Transform", National Conference on Security Issues in Network Technologies August 11-12, 2012

[4]] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. Signal Processing, 66:385–403, 1998

[5] Prof. Manoj Ramaiya Richa Mishra, " Digital Security using Watermarking Techniques via Discrete Wavelet Transform", National Conference on Security Issues in Network Technologies August 11-12, 2012

[6] Gurpreet Kaur, Kamaljeet Kaur, "Image Watermarking Using LSB (Least Significant Bit)", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN:2277 128X, Volume 3, Issue 4, April 2013.

[7] 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, 01 July 2013.

[8] M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermarking and Content Protection. Boston, London: Artech House, INC, 2003.

[9] M. A. T. Alsalami and M. M. Al-Akaidi, "Digital Audio Watermarking: Survey", Proc. 17th European Simulation multiconference,De Montfort UK, pp. 1-14, 2003