IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735. Volume 5, Issue 6 (Mar. - Apr. 2013), PP 41-45
www.iosrjournals.org

A Review of BSS Based Digital Image Watermarking and Extraction Methods

Dr. Sangeeta Jadhav
Prof and Head of Information Technology Department, Army Institute of Technology ,Pune, India

Abstract :*The field of Signal Processing has witnessed the strong emergence of a new technique, the Blind Signal Processing (BSP) which is based on sound theoretical foundation. An offshoot of the BSP is known as Blind Source Separation (BSS). This digital signal processing techniques have a wide and varied potential applications. The term blind is indicative of the fact that both the source signal and the mixing procedures are unknown. One of the more interesting applications of BSS is in field of image data security/authentication where digital watermarking is proposed. Watermarking is a promising technique to help protect data security and intellectual property rights. The plethora digital image watermarking methods are surveyed and discussed here with their features and limitations. Thus literature survey is presented in two major categories-Digital image watermarking methods and BSS based techniques in digital image watermarking and extraction.*

Keywords – *BSP, BSS, Mixing Coefficient, Digital Image Watermarking, Watermark Extraction.*

I. Introduction

Research in image watermarking almost covers all media forms like audio, video, image text, and 3 D model and software codes. A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of the data source by using a specific computer algorithm. There are lot of similarities between information hiding, steganography and watermarking in distribution of electronic document. Information hiding involves the concealment of information so that an observer does not know about its existence. Steganography generally means "covered writing" where communications are carried out in secret. Watermarking is the embedding of content-dependent information. Information hiding covers both steganography and watermarking **[**1**]** .The blind digital image watermarking scheme does not require original image and watermark during extraction process. The watermarked image is viewed as linear mixture of sources *i.e.* original image and watermarks. In the proposed work BSS theory is used to form these linear mixtures in transmitter and blindly retrieve the robust watermark from the mixture in receiver. Thus instantaneous BSS problem is formulated for Digital image watermarking. Independent Component Analysis (ICA) is the most powerful and widely used technique for performing BSS.

In terms of embedding the watermark, there are two main methods. The first is to embed a random binary string into the cover image [2]and the second method is embed a grayscale or binary image watermark into the cover image [3,4]. The second method has the advantages in terms of robustness and copyright protection.

II. WATERMARKING TECHNIQUES

Watermarking techniques can be classifiedas shown in Figure 2.1 according to the application domain, type of document and human perception [5].

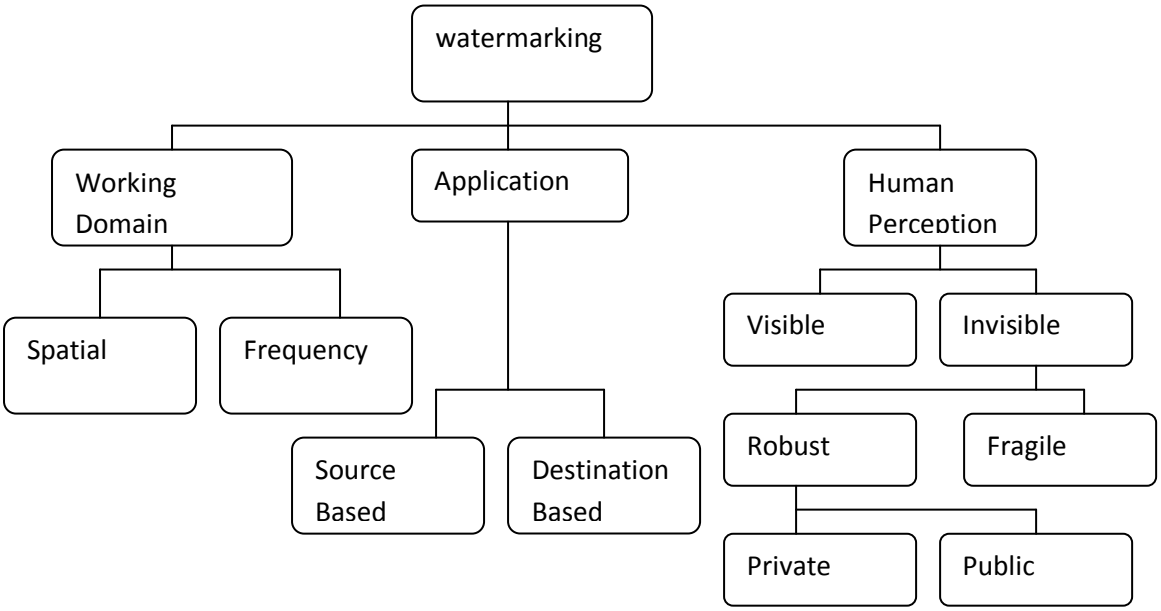

Figure 2.1: Classification of watermark techniques.

There are several ways of classifying watermarking methods as shown in Figure 2.2.4. Most widely adopted classification is based on watermark robustness. Under this classification watermark can be grouped into 3 types

- Robust watermarks :-These watermarks can resist non-malicious distortions[6] Application-wise, robust watermarks are suitable for copyright protection because they can resist common image processing operations
- Fragile watermarks:-These watermarks are easily destroyed by all image distortions. These watermarks can be used to detect tampering and authenticate an image because it is sensitive to changes [7]
- Semi-Fragile:- These watermarks can be destroyed by certain types of distortions while resisting other minor changes. These watermarks are usually applied in some special cases of authentication and tamper detection for example a semi -fragile watermarking scheme [8] for color image authentication using YST color space is presented where embedding space is created by setting the two LSB's of selected sub blocks to zero which will hold the authentication and recovery information

Depending on the availability of the original image, there are three watermark detection/extraction schemes: Non-blind, semi-blind, and blind.

- Non-blind schemes (also called non-public or non-oblivious watermarking) : Both the original image and the secret key(s) are needed
- Semi-blind schemes (also called semi-private or semi-oblivious watermarking) [9]: The secret key(s) and the watermark are needed
- Blind schemes (also called public or oblivious watermarking) [10]: Only the secret key(s) are needed

In nature , the process of watermark embedding is the same as some special kind of patterns or under-written images are added into the host image, we can consider it as a mixture of host image and watermark image, thus without host image the watermark detection is equal to blind source separation in the receiver [11,12].

III. General Watermarking Framework

A watermarking system is usually divided into three distinct steps, embedding, attacks and detection. The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the *host* signal.

1.1.1 Watermark embedding

It is also called watermark encoding. The watermark embedding algorithm embeds a watermark in the spatial and transformed domain of image.

Figure 3.1 shows a generic watermark embedding system. The input parameters for watermark encoder are original image, watermark to be embedded and the secret or public key.

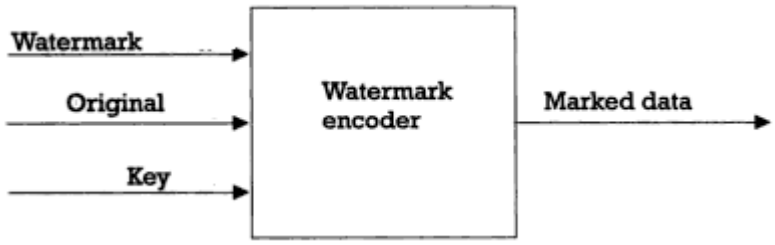

Figure 3.1: Generic Watermark Embedding Scheme

The output of the embedding process is always the watermarked data/image

1.1.2 Attacks

If any person makes a modification in transmitted signal, is called an *attack.*

In watermarking robustness against attacks is a major requirement. An attack is successful if the watermark cannot be detected anymore but the image is still intelligible and can be used for other purposes. With appropriate design objectively high robustness can be achieved. The attacks are classified into four categories

1. Simple attacks–These are conceptually simple attacks which attempt to impair the watermark by manipulation of the watermarked data. Examples include addition of noise, linear and nonlinear filtering, cropping *etc.*
2. Synchronization attacks-These attacks attempt to break the correlation by geometric distortion like rotation zooming *etc.* Watermark recovery becomes impossible for watermark detector due to this type of attacks.
3. Removal attacks- These attacks attempt to separate and remove the watermarks. Examples include denoising the watermarked image through median or high pass filtering.
4. Inversion attacks- Th Inversion attacks- These attacks attempt to confuse by producing fake original data which degrades the authority of watermark by embedding one or several additional watermarks .

3.1.3 Watermark Detection

This is also called extraction of watermark. It is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal. A generic watermark detection scheme shown in Figure 3.2 needs a watermarked data and the secret key or public key.

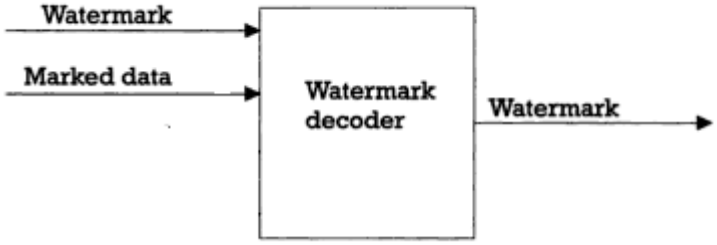

Figure 3.2: Generic Watermark Detecting Scheme

Figure 3.3:

For digital color image watermarking following requirements should be satisfied –

- Elements of digital content can be directly manipulated and information can be embedded in them.
- Watermark should be perceptually invisible. Alterations introduced in the image should not reduce its perceived quality.
- Deterioration of the quality of digital content is minimized.
- Watermarks are retained and detectable after the digital content is edited, compressed, or converted. Thus Watermark should be robust as much as possible against attacks or image processing operations that preserve a desired image quality.
- Processing required for watermarking and detection should be simple.

The Detection of the watermark should not require access to the original image data. This demand is necessary for avoiding time consuming search in large digital image libraries.

IV. Bss In Digital Image Watermarking

Applications of BSS in document security is attracting more researchers because this technique does not require any a-priory information . The application includes the BSS applied at added encryption level and the separation keys are used to control the BSS decryption. Combinations of approaches like combining wavelet fractal with BSS to realize the embedding, detection of watermark to improve the security.

In nature, the process of watermark embedding is the same as some special kind of patterns or under-written images are added into the host image, we can consider it as a mixture of host image and watermark image, thus without host image the watermark detection is equal to blind source separation in the receiver.

Theory of BSS along with RGB decomposition to embed and extract the watermark. By experimentation with various images the mixing matrices are determined by trial and error method[13]. A binary image is embedded into a wavelet approach sub-image. Fast ICA algorithm is used to extract the watermark and fixed mixing matrix is selected for forming watermarked mixtures. Ju Liu, Xingang Zhang *et al.* [14] discusses the watermarking scheme based on the combination of DWT and ICA and a random mixing matrix is used to form the mixtures of images which are used as approximate image of watermarked image and the other as the key. A robust audio watermarking [15] based on ICA and Singular Value Decomposition(SVD) where a random mixing matrix is used.

Spatial methods using BSS are discussed in previous literature like a blind watermark detection using ICA for Spread spectrum based image watermarking [16]. The digital image watermarking in wavelet domain and extraction using MLICA and in embedding a random key is used [17]. The watermark embedding is done in spatial domain using a secret key and extraction adopts ICA[18] where a global histogram approach is used to segment the video and ICA is used for each segment for watermarking.BSS based image watermarking [19] are discussed in previous literatures with fixed or random mixing matrices during embedding.

V. Challenges And Open Issues

Digital watermarking is a complex technology which involve many requirements and tradeoffs. This thesis has handled 3 major open issues regarding digital image watermarking

- Capacity- Related issues include the optimum amount of data, a method to embed and finally the extraction of watermark. In the proposed work the effort is taken to determine the optimum amount of data to be embedded in the cover image using the optimization technique and BSS theory.
- Robustness-This is the main requirement of digital watermarking in applications like copyright protection and content authentication. The presented work has been developed towards the robustness requirement and producing the promising results.
- Transparency- This feature of digital watermarking is required in most of the applications in real world. It is related to the issue of embedding of watermark in such a way that it should not perceptually degrade the data.

5.1. Applications and utility

Digital image watermarking has numerous applications in variety of fields. Some of the application fields are mentioned below.

The main applications fields of digital image watermarking are –

- Copyright Protection

Watermarking can be used to protect redistribution of copyright material over the untrusted network like Internet or peer-to-peer networks.

- Content Archiving

Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video.

- Meta data Insertion

Meta-data refers to the data that describes data. Images can be labeled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Medical X-rays could store patient records.

- Tamper Detection

Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed or degraded, it indicates the presence of tampering and hence the digital content can not be trusted. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery .

- Digital Fingerprinting

Digital fingerprinting is a technique used to detect the owner of the digital content .Finger prints are unique to the owner of the digital content . Hence a single digital object can have different fingerprints.

VI. CONCLUSION

The literature reviewed for digital image watermarking shows that there is lot of scope of improvement in the field of watermarking using Blind Source Separation (BSS). The embedding and extraction of watermark processes may be further modified so as to achieve high degree of imperceptibility and robustness.

Thus the presented work will be useful to develop aBSS based optimized system with variable values of mixing matrix for digital image watermarking.

References

[1] J.J. Eggers, R. Bauml, R Tzschoppe and J Huber, "Applications of Information hiding &digital watermarking" ECDL WS Generalized Documents Yr 2001,pp1-6.

[2] Wong Hon Wah, " Image Watermarking and data Hiding Techniques" Ph D Thesis , Hong-Kong Univ. ,Yr2003,pp1-70.

[3] Dr GN Swamy and B. Surekha, " A Spatial Domain Public Image Watermarking" International Journal of Security and Its Applications, Vol,5 No. 1,Yr 2011,pp 1-11.

[4] S. Radharani and Dr. ML valarmathi , " A Study on Watermarking Schemes for Image Authentication" International Journal of Computer Applications(0975-8887),vol-2-No 4, Yr 2010,pp 24-31.

[5] Peter Foris and DusanLevicky, "Adaptive Digital Image Watermarking Based on Combination of HVS Models" Radio Engineering Vol-18,No-3 Sep 2009,pp 317-323.

[6] Rajesh KannanMegalingam,MithunMuralidharan Nair, Rahul Srikumar ,VenkatKrishnanBalsubramanian and VineethSarma, VenugopalSarma," A Comparitive Study on Performance of Novel Robust Spatial Domain Digital Image Watermarking with DCT based watermarking" International Journal of Computer Theory and Engineering Vol-2,No-4, Yr 2010,pp 1793-8201.

[7] Hua Yuan and Xiao-Ping Zhang, "A Multiscale Fragile watermarkBased on the gaussian Mixture Model in the Wavelet Domain " IEEE proceedings of ICASSP,Yr-2004, pp III-413-416.

[8] M. Hamad Hassan. And S.A.M. Gilani, " A Semi -Fragile Watermarking Scheme for Color Image Authentication" World Academy of Science ,Engg. And Technology, Yr-2006, pp 36-38.

[9] JanuszKusyk and Ahmet M. Eskicioglu, "A Semi- Blind Logo Watermarking Scheme for Color Images by Comparison and Modification of DFT Coefficients",
Google Search: http://*citeseerx.ist.psu.edu*

[10] Xinde Sun and Shukui Bo, " A Blind digital Watermarking for Color Medical Images Based on PCA" IEEE, Yr-2010, pp421-427.

[11] Joachim J. Eggers, Jonathan K. Su and Bernd Girod, "Performance of a practical Blind Watermarking Scheme", proceedings of SPIE Vol 4314 Yr 2001, pp1-12.

[12] Peter H.W. Wong and Oscar C Au and YM Yeung," A Novel Blind Multiple Watermarking technique for Images" IEEE Transactions on Circuits and Systems for video Technology,vol-13,No.8,Yr-2003, pp813-830.

[13] Moilim Amir, AbdellahAdib and DrissAboutajdine, "Color Images Watermarking by Means of Independent Component Analysis",in IEEE transaction , yr-2007,pp 347-350.

[14] Ju Liu, Xingang Zhang and Jiande Sun, " A New Image watermarking Scheme Based on DWT and ICA" IEEE Int Conf. Neural Networks and Signal Processing ,Yr2003,pp 1489-1492.

[15] Xiao-Hong Ma Zhong-Jie Liang and Fu-Liang Yin "A digital audio Watermarking Scheme Based on Independent Component Analysis and Singular Value Decomposition" Proceedings of 5th International Conference on Machine Learning and Cybernetics ,Aug 2006,pp2434-2438.

[16] Hafiz Malik, AshfaqKhokhar and Rashid Ansari, " Improved Watermark Detection for Spread Spectrum Based Watrmarking using Independent Component Analysis" ACM, pp 102-111, Yr 2005.

[17] G. Thirugnanam and S. Arulselvi, " Maximum Likelihood ICA and Kernel ICA comparison for Wavelet Based Digital Image Watermarking", International Journal of Signal and Image Processing,Vol-1-2010/Issue1, Yr-2010,pp 12-17.

[18] SUN Jiande and Liu Ju, "A Blind Video Watermarking Scheme Based on ICA and Shot Segmentation." DOI: 10.1007/s11432-006-0302-9,Science in China: Series of Information Sciences 2006,Vol-49,No-3n302,pp 302-312.Yr-2006

[19] Ren Shijie,SuXin, YuHuishan and Niu Huijuan, " Blind Watermarking Based on Fast ICA and DWT", Proceedings of IWISA 2009,pp 256-259.