International Journal of Research

Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 02 Issue 06
June 2015

Investigation of Adaptive Watermarking Techniques

P.G.V. Suresh Kumar[1], Seelam Sowjanya[2]

[1]*Centre of ITSC, Addis Ababa Institute of Technology, Addis Ababa University, Ethiopia*
[2]*Asst.Professor Depart. of CSE, Priyadarshini Institute of Technology and Science, Chintalpudi, India*
[1]pendemsuresh@gmail.com,[2]seelam.soujanya@gmail.com

ABSTRACT:

Digital media offer several distinct advantages over analog media, such as high quality, easy editing, high fidelity copying. The proliferation of digitized media due to the rapid growth of networked multimedia systems has created an urgent need for copyright enforcement technologies that can protect copyright ownership of multimedia objects. The ease by which digital information can be duplicated and distributed has led to the need for effective copyright protection tools. Various watermarking techniques have been recently introduced in attempt to address these growing concerns. It is done by hiding data within digital audio, images and video files. Various techniques have been developed based on spatial method and Transform methods. In this paper we are evaluating these adaptive watermarking techniques and analyze these watermark techniques. Currently watermark techniques based on the transform domain are more popular than those of spatial domain .In transform domain methods, DWT based method is most widely used because of its robustness against compression and noise.

Keywords**:** Digital water marking, LSB, DCT, DWT.

[1] INTRODUCTION

With the increased use of multimedia data, such as images, video and audio, the concern about intellectual property right (IPR) and data authentication has been raised. Digital Watermarking scheme plays an important role in guaranteeing IPR and data authentication since it provides a mechanism that Hides some information in cover data – images, video, audio and so on. This information is used for IPR and cover data authentication. All watermarking techniques must satisfies three important requirements: perceptual invisibility, robustness against various image processing, such as geometric distortions (rotation, translation, cropping, etc), filtering and compression, and finally ability of watermarking detection without ambiguity. To this end recently many watermarking algorithms have been proposed in the literature. Several methods have been processed in frequency domain; such like DCT, and DWT, and other are processed in spatial domain such as LSB. Especially DWT-based watermarking methods have been researched intensively, due to the fact that the current image compression is based on wavelet domain, such like JPEG 2000.

In this paper, to understand the previous watermark researches and to give help for the future related researches, we try to classify and

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 02 Issue 06
June 2015

analyze the conventional watermark techniques in many ways.

[2]GENERAL FRAMEWORK FOR WATERMARKING

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. A simple example of a digital watermark would be a visible "seal" placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material.
In general, any watermarking scheme (algorithm) consists of three parts.

- The watermark.
- The encoder (insertion algorithm).
- The decoder and comparator

[3] WATERMARK

Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm. Incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object.

[3.1] ENCODING

Following figure illustrates the encoding

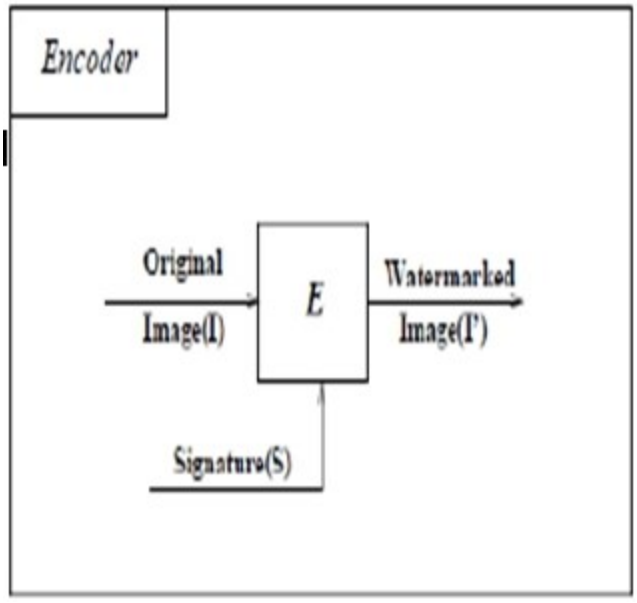

Fig1: Encoder

E is an encoder function, it takes an image I and signature S and generates watermarked image 'I'

[3.2] DECODING

A Decoder D takes an image J, whose ownership is to be determined and recovers a signature 'S' from image. In this process an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 02 Issue 06
June 2015

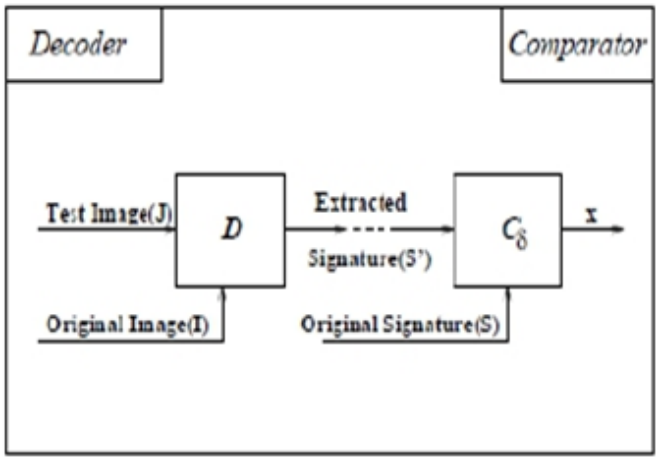

Fig2: Decoder

[3.3] DIGITAL WATERMARKING

Digital Watermarking is the process of embedding a special data into media such **as** image, audio, video and some other data. This embedded information, known as a watermark, can be extracted from the mult imedia contents later and used for supporting the ownership. Embedding watermark can be considered a crucial step for copyright protection and temper proofing. Watermarking can be classified on the following basis:

Classification		Contents
Inserted media category		text, image, audio, video
Perceptivity of watermark		visible, invisible
Robustness of watermark		robust, semi-fragile, fragile
Inserting watermark type		noise, image format
Processing method	Spatial domain	LSB, patchwork, random function
	Transform domain	look-up table spread spectrum
Necessary data for extraction		private, semi-private, public watermarking

Fig 3: Classification of Watermarking

[4] Classification according to human perception

Visible watermark is a secondary translucent overlaid into the primary image. The watermark appears visible to a casual viewer on careful inspection.

The **invisible-robust** watermark is embed in such a way that alternations made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism.

Classification according to robustness of water mark

Robust watermarking: A robust mark is designed to resist attacks that attempt to remove or destroy the mark. Such attacks include lossy compression, filtering, and geometric scaling to improve robustness, it may be necessary to reduce the size of embedded data and embed it multiple times under different parts of selected coefficients here each embedding responds to a particular attack in a different way. Interesting work in robustness was recently reported by [11] (called cocktail) and it is one of few methods claimed to be very robust against variety of attacks.

Semi-fragile watermarking *a* semi fragile watermark lets some changes can be introduced in the watermarked image.

Fragile Watermarking A fragile mark is designed to detect slight changes to the watermarked image with high probability. The main application of fragile watermarks is in content authentication.

[4.1] Classification according to inserting watermark type:

An inserted watermark image can be of two types

Noise type:-Pseudo random noise and Gaussian random sequence

Image Format type:-Binary image, Stamp, logo.

[4.2] Classification according to processing method:

Spatial embedding inserts messages into image pixels, usually in the least significant bits1 (LSB) 2[10]. LSB embedding has the merit of simplicity, but suffers from the lack of robustness. LSB embedding is susceptible to image-processing type of attacks. Error-correct ion coding has been proposed for enhancing the robustness [9][13], but its effectiveness is limited to low levels of noise. If spatial embedding in-volves higher order bits, one runs the very real risk of the steganography being detected.

Transform embedding includes, DCT, FFT, and wavelet transforms are the methods of data transformation. In these methods, a watermark that one wishes to embed is distributed in overall domain of an original data, and the watermark, if it is once embedded, is hardly to be deleted.

The followings present the watermarking methods based on the transform. Most DCT based methods transform 8x8 sized block image into the transform coefficients with the same size. Most energy is concentrated on some coefficients including DC coefficient.

Wavelet-based methods decompose an image into each sub-band. Each band also keeps some information of spatial property. Therefore, the processing time of these methods can be fast by using the multi-resolution characteristic, and a watermark can be inserted into certain sub-bandsite.

[5] DISTORSIONS AND ATTACKS

In practice, a watermarked object may be altered either on purpose or accidentally, so the watermarking system should till be able to detect and extract the watermark. Obviously, the distortions are limited to those that do not produce excessive degradations, since otherwise the transformed object would be unusable. For intentional attacks, the goal of the attacker is to maximize the reduction in these probabilities while minimizing the impact that his/her transformation produces on the object; this has to be done without knowing the value of the secret key used in the watermarking insertion process, which is where all the security of the algorithm lies. Next, we introduce some of the best known attacks. Some of them may be intentional or unintentional, depending on the application:

[5.1] Additive Noise.

This may stem in certain applications from the use of D/A and A/D converters or from transmission errors. However, an attacker may introduce perceptually shaped noise (thus, imperceptible) with the maximum unnoticeable power. This will typically force to increase the threshold at which the correlation detector works.

[5.2] Filtering.

Low-pass filtering, for instance, does not introduce considerable degradation in watermarked images or audio, but can dramatically affect the performance, since spread-spectrum-like watermarks have a non-negligible high-frequency spectral contents.

[5.3] Cropping.

This is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of a video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place.

[5.4] Compression.

This is generally an unintentional attack which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark insertion task in the same domain where the compression takes place. For instance, DWT domain image watermarking is more robust to JPEG compression than spatial-domain watermarking.

[5.5] Rotation and Scaling.

This has been the true battle horse of digital watermarking, especially because of its success with still images. Correlation based detection and extraction fail when rotation or scaling are performed on the watermarked image because the embedded watermark and the locally generated version do not share the same spatial pattern anymore. Obviously, it would be possible to do exhaustive search on different rotation angles and scaling factors until a correlation peak is found, but this is prohibitively complex. Note that estimating the two parameters becomes simple when the original image is present, but we have augmented against this possibility in previous sections. In[7] the authors have shown that although the problem resembles synchronization for digital communications, the techniques applied there fail loudly. Some authors have recently proposed the use of rotation and scaling-invariant transforms (such as the Fourier-Mellin[8] but this dramatically reduces the capacity for message hiding. In any case, publicly available programs like Strirmark break the uniform axes transformation by creating an imperceptible non-linear re sampling of the image [6] that renders invariant transforms unusable. In audio watermarking it is also quite simple to perform a non-linear transformation of the time axis that considerably difficult watermark detection.

[5.6] Statistical Averaging.

An attacker may try to estimate the watermark and then "unwatermark" the object by subtracting the estimate. This is dangerous if the watermark does not depend substantially on the data. Note that with different watermarked objects it would be possible to improve the estimate by simple averaging. This is a good reason for using perceptual masks to create the watermark.

[5.7] Multiple Watermarking.

An attacker may watermark an already watermarked object and later make claims of ownership. The easiest solution is to timestamp the hidden information by a certification authority.

[5.8] Attacks at Other Levels. There are a number of attacks that are directed to the way the watermark is manipulated. For instance, it is possible to circumvent copy control mechanisms discussed below by super scrambling data so that the watermark is lost [9] or to deceive web crawlers

searching for certain watermarks by creating a presentation layer that alters they way data are ordered. The latter is sometimes called "mosaic attack" [6].

[6] COMPARISON OF DIFFERENT WATERMARKING TECHNIQUES AND EFFECT OF ATTACK:-

LSB embedding has the merit of simplicity, but suffers from the lack of robustness. LSB embedding is susceptible to image-processing type of attacks. As comparison have been made in early researches by calculating the threshold value introducing different attacks on spatial and transform methods:-

Compression

Realizing the JPEG compression on different watermark images[2] it is calculated that DWT shows minimum effect of it.

Contamination by Gaussian noise[2]

In DWT robustness of the algorithm is effected introducing Gaussian noise to watermarked image is more in LSB as compare to DWT. In DWT the noise density used in simulation is from 10% to 50%.

Clippings[2]

The clipping of a part of the image of the watermarked image is realized. All cases detector detect correctly embedded watermark in DWT.

Geometric Distortion

Effect of geometric distortion is also negligible in DWT. The results obtained by [2] show that the presented methods DWT satisfy perceptual invisibility and it is sufficiently robust, due to that the embedded watermarks already survive over the different type of attacks. However the algorithm shows it's vulnerability against JPEG compression, the detector can't detect the watermark from compressed watermarked image with quality factor 60. To achieve more robustness and perceptual invisibility in the method, it is necessary to investigate on the relation between the coefficients Wavelet and the HVS in a deeper way.

CONCLUSION

In this paper, we tried to classify and analyze many previous watermarking methods based on spatial and transform techniques. We classified the previous works the various points of view: the inserted media category, the perceptivity, the robustness, the baseband, the visible, invisible or dual watermarking type, the inserting watermark type, the processing method and the necessary data for the watermark extraction. Most of researches handled the watermark techniques on image media. Invisible watermarking, robust watermarking, JPEG compression and noise style embedding have been main issues in the previous researches. In terms of processing domain, transform domain has been used rather than the spatial domain. Earlier DCT-based approach was widely used, but now with the development of DWT emphasis is given on the wavelet domain approaches, wavelet-based approach which has the multi-resolution characteristic, is getting its popularity day by day.

FUTURE SCOPE

With the broad spreading of internet, audio and video based services such as MP3 and VOD are also being widely used. Therefore, proper audio and video watermarking techniques are also required to study intensively.

REFERENCES

[1] A. Tirkel, et al., "*Electronic Water Mark,*" In Proc. ,DICTA, pp.666-672, 1993.

[2] íctor V. Hernández Guzmán; Mariko Nakano Miyatake; Héctor M. Pérez Meana " Analysis of Wavelet based watermarking Techniques" 2004, IEEE.

[3] A.P.Petitcolas,Ross J.Anderson and Marhs G.Kuhn, "*Information Hiding-A Survey Fabien* ", Proceedings of the IEEE, 87(7):1062--1078, July 1999.

[4] C. Podilchuk, W. Zeng. "*Image-adaptive watermarking using visual models"*. IEEE J. Select. Areas Commun. 1998, 16(4):525-539

[5] Wang H-J M, Su P-c, Kuo C-C J. "*Wavelet-based digital image watermarking*". Optics Express, 3(12): 491- 496, 1998.

[6] Petitcolas, R. Anderson, and M. Kuhn, "Attacks on copyright marking systems," in *Information Hiding* (D. Aucsmith, ed.), vol. 1525 of *Lecture Notes in Computer Science*, (Berlin), pp. 218–238, Springer- Verlag, 1998.

[7] J. R. Hern´andez, F. P´erez-Gonz´alez, and J. M. Rodr´ıguez, "Coding and synchronization: A boost and a bottleneck for the development of image watermarking," in *Procof the COST #254 workshop on Intelligent Communications*, (L"Aquila, Italia), pp. 77–82, SSGRR, June 1998.

[8] A. Herrigel, J. O"Ruanaidh, H. Petersen, S. Pererira, and T. Pun, "Secure copyright protection techniques for digital images," in *Information Hiding* (D. Aucsmith, ed.),vol. 1525 of *Lecture Notes in ComputerScience*, (Berlin), pp. 169–190, Springer-Verlag, 1998.

[9] I. J. Cox and J.-P. M. G. Linnartz, "Some general methods for tampering with watermarks," *IEEE J. Select. Areas Commun*,vol. 16, pp. 587–593, May 1998.

[10] Y.J. Song, T.N. Tan "*Comparison of Four Different Watermarking Techniques* "Proceedings of ICSP 2000

[11] Lu, C., Huang, S., Sze C. & Liao, H. \Cocktail watermarking for Digital Image Protection" TR-IIS-99-008.