DIGITAL IMAGE WATERMARKING IN WAVELET DOMAIN USING CHAOTIC SEQUENCE

Sumit Pathak[1], Sumit Tiwari[2], Saurabh Agrawal[3]
[1]Asst. Prof.,Department of Computer Science, IPS-CTM Gwalior, India
[2,3]P.G. Scholar,CSE Dept..SRCEM Banmore, M.P. India
Email:sumitpathakcs@gmail.com[1], sumitgwalior23@gmail.com[2], toc.saurabh@gmail.com[3]

Abstract
This paper introduce a method for digital watermarking based on discrete wavelet transform (DWT) using chaotic sequence as a spreading signal. Chaotic sequences are generated through chaotic map, which is determined by initial condition and parameters. The underlying system use wavelet transform to convert original cover image from spatial domain to frequency domain and employs chaotic sequence to spread the watermark over wavelet coefficient. A large number of uncorrelated, random-like, yet deterministic chaotic sequences can be exploited to add the original watermark image to original image .In this type of watermarking the size of original watermark is less than the size of wavelet coefficient. Size of watermark image is made equal to size of wavelet coefficient by chaotic sequence mapping and embedded into the high frequency sub-band of original image. The coefficients whose energies were fewer than the others were selected to hide watermark.

Keywords—Digital watermarking, Wavelet transform, Chaotic sequence.

I. INTRODUCTION

Digital watermarking can be used to insert invisible data into an object helping to track down pirate copies and to prove rightful ownership in a dispute. In principle, watermarking technologies can be applied to any kind of multimedia object, however to achieve the best possible results schemes are normally optimized on a particular medium. The term Digital watermark was first used by Komatsu and Tominaga in 1988[1]. However it was in 1954, Emil Hembrooke of the Muzac Corporation filed a patent for watermarking music works [2]. Since that time, a number of watermarking technologies have been developed and deployed for a variety of applications. Interest in embedded signaling continued throughout the next 35 years. For example, systems were developed for advertisement verification and device control. However, digital watermarking did not receive substantial interest as a research topic until the 1990's. In the first half of that decade, interest in the topic expanded rapidly and today entire conference proceedings are devoted to the subject. In later half of the decade, there was an explosion of interest in digital systems for the watermarking of various content[3].The digital watermarking can be applied to many digital media objects like, image, audio, video, three – dimensional model, executable code, IC's etc. The proposed applications of these methods are many and varied, and include identification of the copyright owner, indication to recording equipment that the marked content should not be recorded, verification that content has not been modified since the mark was embedded, and the monitoring of broadcast channels looking for marked content.

II. THEORETICAL BACKGROUND

A) General model of watermarking

Water marking is processes for embedding the one information into other information. And digital image watermarking can be defined as processes of embedding the image into other

image. The image in which image is embedded is known as cover image and the image which is used to embed, is known as watermark.

A Watermarking processes can be composed of the three parts.

- Watermark
- Encoding processes (insertion algorithm)
- Decoding processes (extraction algorithm)

Watermark can be different for different owner. In other word each user has a unique watermark or an owner can also add different watermark in different cover image. The verification algorithm authenticates the object determining both the owner and the integrity of the object.

1) Insertion Process(Encoding)

For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data W. A block general diagram of this process is shown below.

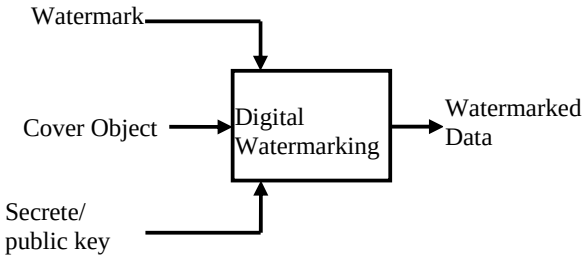


Fig 1 Digital watermarking – Imbedding

2) Extraction Process

Extraction employ watermarked image as a input, cover image used in encoding process and same secrete/public key. The output of this process is recoverd watermark. A block general diagram of this process is shown below.

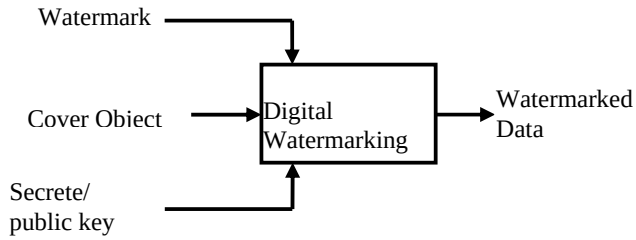


Fig 2 Digital watermarking – Extraction

B. Basic watermarking technique

Watermarks do not always need to be hidden. Watermarking can be broadly classified in two categories:

- Visible watermarking technique
- Invisible watermarking technique

1) Visble watermarking

Visible watermarking was the first and most primitive way of watermarking. In this method the cover object is taken and the watermark in added on it. This makes the watermark visible on the cover object. This was good for identification purposes.

Visible watermarks were created by using Lena's images as the cover images. These images were 8-bit gray scale images. The watermark was chosen as a monochrome image exactly of the same size as the cover object. The watermarked image was achieved by changing the pixel intensity values in the cover image corresponding to white pixels in the watermark. This type of watermarking could only be used for owner identification purposes. For all other applications invisible watermarking is used. An example of visible watermarking is shown in fig 3.

(a) (b) (c)

Fig 3 (a) Leena 256*256, (b) watermark image, (c) watermarked image

Most of the literature has focused on the invisible digital watermarking as it has more application in today's digital world. Visible digital watermarks are strongly linked to the original paper watermarks that have been traced back to the end of 13th century [2].

1) Invisble watermarking

In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some

amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals. Invisible watermarking can be classified on the basis of their working domain.

- Spatial working domain watermarking
- Frequency working domain watermarking
- Wavelet working domain watermarking

A) Spatial working domain watermarking

Watermarking techniques can be broadly classified into two categories. They are spatial domain watermarking and frequency domain watermarking. In spatial domain watermarking technique, watermark message is added in to spatial domain. In this type of watermarking we do not perform any image processing operation on host image. We directly perform watermarking operation between pixel of message image and pixel of cover object. Spatial domain watermarking technique are simple and computationally efficient, because they modify the color, luminance or brightness values of a digital image pixels, therefore their application is done very easily, and requires minimal computational power. Example of such type of method is Least Significant Bits watermarking (LSB).

The simplest technique used for hidden watermarking is to hide the message bits in the Least Significant Bits (LSB) of the cover object. The advantage with this method is that even if a part of the stego image is cropped the receiver can still get the required message, as the message is embedded a number of times. The message for this case is considered to be very small as compared to the cover object.

B) Frequency working domain watermarking

Watermarking can be applied in the frequency domain by first applying a transform like discrete cosine transforms (DCT). In a similar manner to spatial domain watermarking, the values of chosen frequencies can be altered from the original. Since high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies that contain important information of the original picture. Since watermarks applied to the frequency domain will be dispersed over the entirety of the spatial image upon inverse transformation, this method is not as susceptible to defeat by cropping as the spatial technique. However, there is more a tradeoff here between invisibility and decodability, since the watermark is in effect applied indiscriminately across the spatial image. DCT based watermarking is example of this type of watermarking.

In DCT domain watermarking, we first perform discrete cosine transform on cover object and then we embed watermark in to transform image. Frequency domain watermarking involves computation of the DCT of the pixel matrix of both the image as well as the watermark to be embedded on it. Then DCT coefficients are scaled and added. Finally the resulting DCT coefficients are subjected to IDCT. Here we can observe that in frequency domain watermarking, lot of complex logic is involved.

III. PROPOSED METHOD FOR EMBEDDING DIGITAL WATERMARK

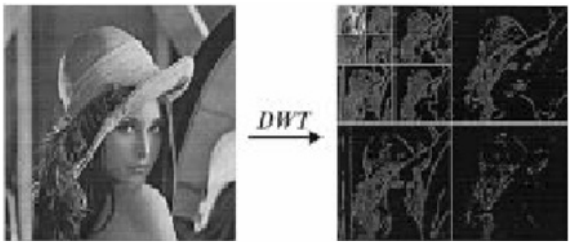
A) Wavelet transform

According to Rehmi Post in [4], a wavelet transform is a “tool for carving up functions, operators, or data into components of different frequency, allowing one to study each component separately." In more **practical terms** this means that a wavelet transform decomposes a signal into windows of different resolutions.

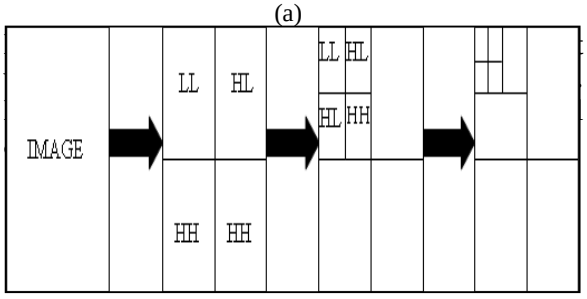
For doing so, a wavelet transform applies a wavelet on the (one-dimensional) data of interest resulting in a multiresolution signal representation. This is done by separating the signal and details at a frequency determined by the wavelet and then keep repeating this on the low frequency output of this operation until some condition is met (e.g. the signal has become too small to be split again). Like other linear transforms on the space of real/complex valued functions, the wavelet transform is a change of basis. This is similar to e.g. the

Fourier series, only that instead of using the base functions sine and cosine functions wavelets are used. The signal to decompose can be continuous (e.g. functions) or discrete (e.g. images), and thus we distinguish between the continuous wavelet transform (CWT) and the discrete wavelet transform (DWT).

An Image can be represent on multiple resolutions, which are called multiresolution analysis (MRA). Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error. The fact that wavelet-based data structure has been adopted in the established image coding standard JPEG200 encouraged extensive watermarking study in wavelet transform. Wavelet transform separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail comments.



(a)



(b)

Fig 3 (a) Wavelet Transforms of Image (b) Multidimensional Wavelet Transforms

B) *Properties of wavelet transform*

Depending on the target application, a wavelet is characterized by a number of properties. Some of these considered relevant for image processing applications are:

Compact support means that a wavelet's values are zero outside a bounded interval. Wavelets with compact support are usually said to have good time or space localization properties.

Smoothness is responsible for good approximation at coarser detail levels; the lack of it usually leads to blocky and/or edgy artifacts.

Filter length determines over how many wavelet coefficients a single signal value is distributed in the transform domain. This is of interest for applications like image compression or watermarking where the signal is manipulated in the transform domain.

C) *Application in Image watermarking*

The DWT (Discrete Wavelet Transform) [8] separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown below in Fig. 6. One of the many advantages over the wavelet transform is that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image qualitynot use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you?

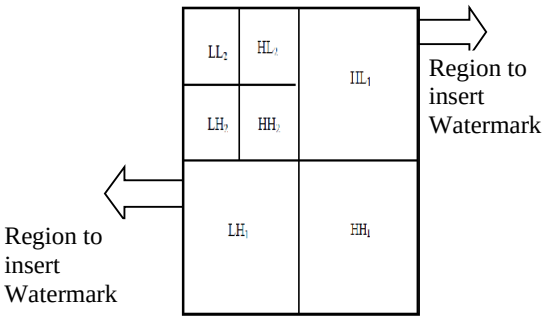


Fig4 Sub Band Theory of Wavelet Transforms

D) *Chaotic sequence*

A chaotic system is a deterministic dynamical system whose states change with iterations in a deterministic way *[U]*,i. e., a nonlinear dynamical system model based on its *N* previous values can be described as

$$\mathcal{C}_n = f(\mathcal{C}_{n-1}, \mathcal{C}_{n-2}, \mathcal{C}_{n-3}, \ldots\ldots\ldots, \mathcal{C}_{n-N}, \alpha)$$

Where, A is the bifurcating parameter. A chaotic system generates a set of aperiodic signals with a "noise-like" and broad power spectrum. The system is very sensitive to initial conditions. A slight difference in initial conditions will produce totally different sequences, which possess good correlation properties [5].

These characteristics of a chaotic signal are very helpful in digital watermarking applications. The noise-like and wideband output of a chaotic system can be used as the spreading sequence to spread out copyright information. Because of the good correlation properties of chaotic signals, the inserted information can be retrieved properly when the correlation detector is applied. Furthermore, the correlation of certain chaotic spreading sequences is close to the optimal correlation performance for the application of image watermarking. Thus, it is reasonable to expect that using chaotic spreading sequences is superior to widely used classical spreading sequences, such as m-sequences and Gold sequences in terms of robustness and security.

A) Watermarking Using Chaotic Sequence

A large number of uncorrelated, random-like, yet deterministic signals can be generated in the interval of $(-1,1)$ by executing the logistic map equation recursively. And quantization of these numbers also does not destroy the desirable properties of these kinds' sequences [7].

Encoding: To embed or to encode watermark in to cover object, first we transform the cover object from spatial domain to frequency using wavelet transform and calculate wavelet coefficient. Ann embedding process can be done according to equation.

$$I_W(x,y) = I(x,y) + k \times W(x,y)$$

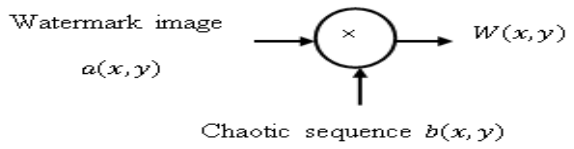
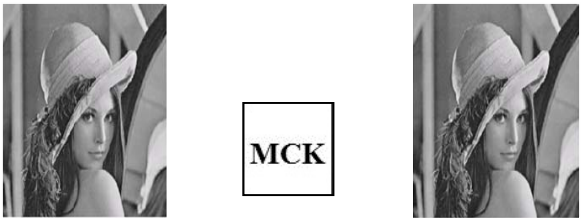


Fig Embedding Process



(a) (b) (c)

Fig (a) Cover Image, (b) Watermark Image, (c) Watermarked Image

Decoding: To recover the original watermark $a(x,y)$, the watermarked image $I_W(x,y)$ is multiplied at the receiver again with a pseudonoise sequence which is an exact replica of that used for embedding the data.

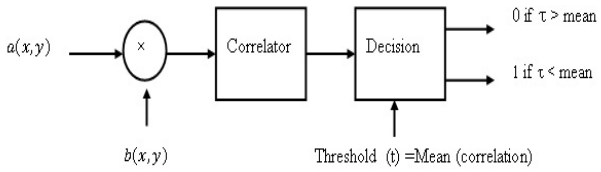


Fig Decoding Process

Fig describes the block diagram of watermark extraction process. Same chaotic sequences that have been used in embedding process, generated $a(x,y)$ by logistic map.

$$C = I_W(x,y) \times b(x,y)$$
$$= (a(x,y) \times b(x,y) + I(x,y) \times b(x,y)$$
$$= a(x,y) \times b^2(x,y) + I(x,y) \times b(x,y)$$

The above equation shows that the watermark image $a(x,y)$ is multiplied twice with the noise signal $b(x,y)$, whereas the unwanted or the cover image $I(x,y)$ is multiplied only once with the noise signal. So $b^2(x,y)$ becomes 1 and the product $I(x,y) \times b(x,y)$ is the unwanted noise signal that can be filtered out during the process of correlation by setting the threshold as mean of correlation. Hence, at the receiver we recover the watermark image $a(x,y)$ [6].

a) (b) (c)

Fig (a) Watermarked Image, (b) original Watermark, (c) Recovered Watermark

IV. CONCLUSION AND FUTURE WORK

This paper presents the technique of image watermarking using chaotic sequence. The chaotic sequences are distinguished by their wideband, noise-like, nonlinear characteristics, simple generation and storage these sequence show zero cross correlation, and low auto correlation since these sequence is very sensitive with respect to their initial condition

which could be useful in the recovery of watermarks by using spread spectrum techniques. The watermarked images and the PSNR obtained using the proposed method ensures robustness and quality of the watermarked image. It has proven that chaotic sequence provides improvement in the value of PSNR for watermarked image. Hence the method can serve as a suitable substitute for other algorithms available at present. Digital Watermarking has many objectives in image watermarking like authentication, owner identification, copy control, Fingerprinting, data authentication and many more. This thesis presents a watermarking technique for gray scale image. This work can be extended to embed watermark in to colour image and it can be further extended to imbed watermark in video film. Since video film is composed of multiple frames or multiple images so having embedded watermark in one image we could also embed watermark in to multiple images one after one or simultaneously. And we can serve the various objectives of image watermarking for video watermarking also.

References

[1] I.J. Cox, M.L. Miller, and J.A. Bloom, "digital Watermarking", Morgan Kaufmann Publishers 2002.

[2] S.Katzenbeisser, Petitcolas, F.A.P, "Information hiding techniques for steganography and digital watermarking", Artech House Publishers, 2000.

[3] M.Gnanaguruparan, "Recursive secret sharing in visual cryptography", MS thesis, Louisiana State University.

[4] http://cpk.auc.dk/dicom/Eo2/*CDMA*.htm

[5] Devaney R.L., "An Introduction to Chaotic Dynamical Systems", Wesley Publishing Company, Inc., California, 1989.

[6] Siyue Chen, "Chaotic Spread Spectrum with Application to Digital Image Watermarking", MS Thesis, University of Calgary.

[7] S.Haykin, "Communication Systems", *4th edition, John Wiley and Sons, Inc, 2001*.

[8] M.D.Swatson, B.Jhu, A.H.Tewfik, "Transparent robust image watermarking", Department of Electrical engineering,University of Minnesota.