UDC 004.932

Abdinurova N.R. [1], Tolebi G.A. [2]

[1] MSc in Computer Science, lect., *Suleyman Demirel University, Kaskelen, Kazakhstan*
e-mail: nazgul.abdinurova@sdu.edu.kz
[2] MSc in Robotics, lect*., Suleyman Demirel University, Kaskelen, Kazakhstan,*
e-mail: gulnur.tolebi@sdu.edu.kz

WATERMARKING AND COMPARISON OF THE TWO SPECIES

Abstract. Watermark is the piece of information inserted into data for the copyright protection. Two technologies of watermarking: LSB and DWT will be explained and compared below .

Key words: LSB, DWT, robustness, spatial domain

1. Introduction

The immense popularity and expeditious widening of the Internet show the commercial potential of proposing digital data through the networks. Since commercial interests mean a chance to make a profit, the authors and creators are concerned about protecting their ownership rights. Digital watermarking can be explained as one of the possible and effective approach for defending intellectual property.

A digital watermark is a digital signal or pattern inserted in order to identify copyright information. It is embedded information data within an insensible form for human visual system but in a way that protects from attacks such as common image processing techniques.

As well as, watermarks can be inserted into papers (hard copies) by varying its thickness when it is manufactured. There are many other special properties in use, such as fluorescent threads. An extreme example is the Australian $10 note, which is printed on plastic and has a see through window.[1,2] Since this essay is more concerned about digital watermarking from a cryptographic perspective, some ways how the ownership of digital data can be protected will be discussed below.

2.1 Basic on watermarking

Digital watermarking can be contrasted against public-key encryption, though it has quite a lot of differences. Encryption is used mostly for messages that are involved in a communication. The encryption procedure changes the messages completely and the original message can only be retrieved by decryption. And once the message is decrypted, there are no residues left on the message. But in case of Digital watermarking, a permanent signature is left on the digital data (like music, movies and photos) so that the ownership can be verified later on using special software. Also, the digital data can be perceived by anyone as there is no need to decrypt the data to view/read it, i.e. it can be used or re-transmitted. [3]

In Figure 1 you can see general scheme of watermark insertion and detection.

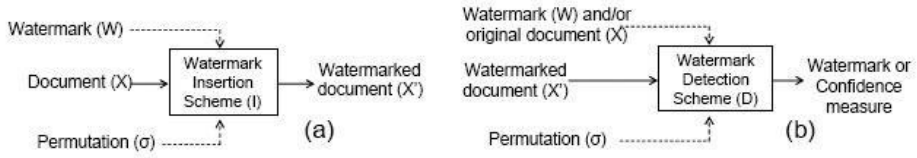

Figure 1: The Processes for (a) Watermark Insertion and (b) Watermark Detection

1.1 Watermarking Requirements

First of all, the requirements of watermarks are defined to provide maximum protection of intellectual property.

Imperceptible

In terms of watermarking, imperceptible refers to the original data's quality which must remain intact or unaffected by the watermark. For a digital data to be imperceptible, the watermark must be embedded in a transparent manner. For example, the hearing or viewing experiences of a photo or music must not be affected by its watermarks.

Undeletable

Ideally watermark should be impossible to remove, at least to be difficult to delete without obviously degrading the host signal.

Statistically Undetectable

A "pirate" should not be able to detect the watermark by comparing several watermarked signals from one sender.

Robustness

The watermark should survive any compressions or other operations applied to it causing lot of data or quality, like converting an image to JPEG.

Unambiguous

Retrieval of the watermark should be unambiguously identify the owner, and the accuracy of identification should degrade gracefully in the face of attack

Capacity:

Watermark's capacity refers to the amount of watermark information that can be applied to the host/original data.

2.2 Types of Watermarks

Watermarks and watermarking techniques can be distinguished in various ways. According to visibility we can classify digital watermarks into 2 types:

1. Visible
2. Invisible

A visible watermark is a viewable or noticeable watermark that is imprinted over the original data. It is stronger and more robust in nature, and as a result is often preferred more to apply strong copyright protection on digital data. On picture below you can see example of visible watermark:

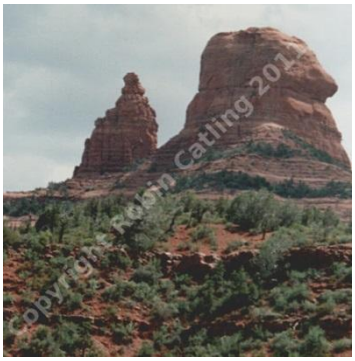

Figure 2

An invisible watermark is an embedded image which cannot be perceived with human's eyes. Only electronic devices (or specialized software) can extract the hidden information to identify

the copyright owner. Invisible watermarks are used to mark a specialized digital content (text, images or even audio content) to prove its authenticity [4].

2.3 Watermarking Techniques

2.3.1 Spatial Domain

Watermarks also can be divided according the techniques used to embed them. For example, there are number of ways that enable watermarking in the spatial domain. The easiest way for many programs is to use least significant bit method.

Least significant bit

Now let's describe technique of applying this method on images. Since image is the two dimensional array of pixels, watermark will be embedded on that pixels. First of all, we have to convert pixels (because in rgb format there 3 values for every pixel) into greyscale then perform our operation on least significant bit (LSB) of each pixel. Knowing obviously limitations of HVS we can conclude that processing of small difference in the LSB will not be noticeable.

The steps to embed watermark image are given below.

A. Steps of Least Significant bit

1) The image is first converted into greyscale from RGB format
2) The double precision is then applied on the image
3) The most significant bits are shifted to the least significant bits of the image
4) Make least significant bits of host image to zero
5) Add shifted version (step 3) of watermarked image to modified (step 4) host image.

B. Limitations of Spatial Domain Watermarking

This method seems simple and effective, also it can survive transformations such as cropping, any addition of noise. Disadvantage is that knowing about algorithm, everyone can change least significant bit, thereby delete the watermark. For example, if you set all LSBs of watermarked image to '1's, image loss its watermark, but like in case of embedding it this will not be noticeable for human eyes. [5]

2.3.2 Frequency Domain

Another method of watermarking image and do it with high quality is applying watermarking in the frequency domain (and other transform domains). It is performed by transforming with the Fourier, Discrete Cosine Transform (DCT) or Discrete Wavelet transform (DWT) methods. Such as in spatial domain watermarking, the values of chosen frequencies will be changed in the original image. Since compression or scaling can lead to losing high frequency values, the watermark signal should be applied to frequencies with lower value, or of it's possible to perform, applied a to that frequencies which contain substantial information such as edges of the original picture. Watermarks applied to important values of image will be scattered over whole image, which means technique is not amenable to beating as spatial domain method.[6]Now, let's look at one of methods of this technique, explained above.

Discrete wavelet transform watermarking

In the DWT the main idea of watermarking for image is to decompound the image into sub-image of sundry spatial domain and independently on value of frequency. Then alter the coefficient of sub-image. After DWT transforming the original image, we will decompose it into 4 frequency fractions where one low-frequency (LL) and three high-frequency parts (LH, HL, HH). If the information of LL district is DWT transformed, the sub-level frequency region information will be obtained. The number of how many times we decomposed LL district will define level of DWT. Figure 3 shows us example of two-dimensional image after DWT decomposing 3 times. (It is called applying 3rd level DWT)

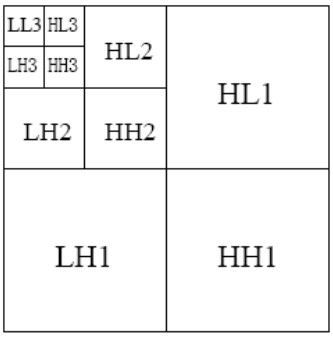

Figure 3

The information of low frequency part is an image nigh to the host image and most signal information of original image is in LL. According to the character of Human Visual System, our eyes are sensitive to the see minuscule change of edge, outline and strip. Thus, it's difficult to conscious that putting the watermarking signal into the big amplitude coefficient of high-frequency band of the image DWT transformed. Then

it can carry more watermarking signal and has good concealing effect

3.1 Watermark Embedding using DWT:

The Procedure of watermark embedding is shown in fig.4

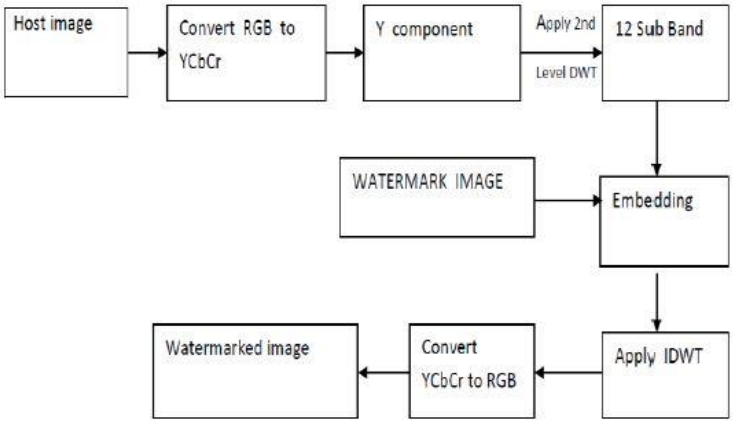

Figure 4

Steps of watermark embedding using DWT method:

1. Convert it from RGB format to YCbCr
2. Apply 2nd level DWT
3. Embed the watermark components in to the frequency subcomponents.
4. Apply IDWT.
5. Convert YCbCr to RGB.
6. Get watermarked image
7. Check Authentication. [7]

3. Conclusion

In this paper we first try to explain what watermarks are and the aim of using them: watermarks are some signal embedded into original data in order to show and prove authority. Watermarks have some requirements such as robustness, imperceptibility and so on. We determine types of watermarks and techniques of watermarking in spatial and frequency domains. In order to compare them we elucidate LSB and DWT methods and list steps of performing them. Now we can conclude that in case of robustness DWT watermarking is comparatively much better than the LSB, since in DWT watermark is embedded into sub-image, which makes watermark stronger for altering or removing. But in case of cost, LSB is computationally cheaper, since there is less number operations should be performed.

References:

1 Ross Anderson, (2001). Security Engineering: A guide to Building Defendable Distributed System. p247, USA: “Wiley Computer Publishing”.(0471389226)

2 http://en.wikipedia.org/wiki/Australian_ten-dollar_note

3 http://www.computerweekly.com/feature/White-Paper-Digital-watermarking

4 Sk.Shamshad , K.L.Sailaja, P.Rameshkumar, Encryption of Watermarked Images using Chakra Symmetric Key Approach, November 2013 International Journal of Advanced Research in Computer Science and Software Engineering, Available at: http://www.ijarcsse.com/docs/papers/Volume_3/11_November2013/V3I11-0109.pdf

5 Darshana Mistry (2010) *Comparison of digital watermarking methods,* September 2010, (IJCSE) International Journal on Computer Science and Engineering,Available at: http://www.researchgate.net/profile/Darshana_Mistry/publication/50235154_Comparison_of_Digital_Water_Marking_methods/file/d912f50f510ef83de1.pdf

6 Mahmoud El-Gayyar (2006)*Watermarking Techniques Spatial Domain Digital Rights Seminar*, May 2006, Media Informatics University if Bonn Germany, Available at: http://wob.iai.uni-bonn.de/Wob/images/55867298.pdf [Accessed on: 15 March 2014]

7 PravinM.Pithiya, H.L.Desai(2013) *DWT Based Digital Image Watermarking, De-Watermarking & Authentication,* June 2013, International Journal of Engineering Research and Development, Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.415.8220&rep=rep1&type=pdf

УДК004.421.5 А28

Aitbayev Y.K.[1], Kabulov B.M. [2], Amirgaliyev Y.N.[3]

[1] *MSc, International Information Technology University, Almaty, Kazakhstan*
e-mail: mansure1991@gmail.com
[2]*MSc,International Information Technology University, Almaty, Kazakhstan*
e-mail:kaboul777@gmail.com
[3] *Prof. Dr. Ing., Suleyman Demirel University, Kaskelen, Kazakhstan*
e-mail:amir_ed@mail.ru

ENSEMBLE LEARNING ALGORITHMS IN PATTERN RECOGNITION TASKS

Аннотация. Статья посвящена теме использования моделей коллективного принятия решений в автоматизированных интеллектуальных системах. Рассматривается применение данных моделей для решения задач распознавания образов. Под коллективным распознаванием подразумевается задача использования множества классификаторов, каждый из которых принимает решение о классе одной сущности с последующим согласованием решений с помощью некоторого алгоритма.

Ключевые слова: распознавание образов, групповые решения, коллективный анализ, интеллектуальные системы

1. Introduction

The current degree of technological and scientific progress requires a focused development of computer vision systems as an important mechanism of providing effective interaction between machinery and humans. One of the most important areas of computer vision is pattern recognition. Successful solution of pattern recognition tasks is necessary to develop systems capable of intelligently evaluating the environment and doing certain actions.

There has been growing interest in pattern recognition tasks in the last decade. This is determined by the prevalence of the problems that is being solved in recognizing images and