www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242

Volume 3 Issue 1, Jan 2014 Page No. 3655-3659

A RESEARCH REVIEW ON DIFFERENT DATA HIDING TECHNIQUES

Dr.K.Sathiyasekar, S.Karthick Swathy Krishna K S

Professor, Department of EEE S.A Engineering College, Thiruverkadu Chennai, India

Assistant Professor, Department of EEE The Kavery Engineering College Salem, India

Post Graduate Student, M.E (Embedded systems) The Kavery Engineering College, Salem, India.
kswathy91@yahoo.com

Abstract*: Data transmission needs security. Data hiding can be achieved through many methods. Different data hiding techniques are discussed in this paper which includes watermarking, steganography, fingerprinting, cryptography and digital signature. Since internet provides images, audio and video in digital form, distributing copies of copyright material are avoided by adding data hiding methods.*

Key words *: data hiding, watermarking, steganography, cryptography*

1. Introduction

In this particular topic it is dealt with image processing techniques and the security that is needed for hiding the data in order to keep the secrecy up to the standards. Image processing is any form of signal processing in which input is an image which can be a photograph or video frame. Likewise the output can be an image or it can be a set of parameters related to the image in which the receiver should be capable to read out."Image'' in computer language means a two dimensional picture and is treated as a function of two variables. A suitable example is CON(x, y) where CON is contrast of the image at coordinates x and y. The image is treated as a 2 dimensional signal and standard signal processing techniques are applied to it for encoding and decoding the image. Normally image processing techniques are considered only as digital image processing. But this is a misconception as image processing can be done by optical or analog methods if needed. The acquisition of images is called as imaging. Advancements have been made for multi dimensions later, which can be achieved by three steps which are:-

- Processing of image-which is a simple image in image out technique
- Analysis-where the measurements of the image out are got.
- understanding-high level description out for the image.

By image processing any images can converted into a digital form and with the help of new technology the image can be enhanced and can even get useful information from it.

Detailed steps are given below-

- To make the partially visible or hidden objects clear
- To sharpen and restore the image
- To retrieve the image
- To take proper measurements of pattern
- To distinguish each objects in an image

"Security'' is of prime concern as the processed image should not be leaked or third party accessed in any way and to keep it confidential if needed. It is classified into two types-Steganography and steganalysis. Steganography is based on embedded technique and steganalysis is based on detection technique. Steganography hides images in the cover of something else. JPEG is the format commonly used for hiding as it is the commonly used file in internet. Files are compressed and encrypted again to up the level of secrecy.

2. Watermarking

2.1 Introduction

A watermark can be explained as an information that is embedded into data for detection of tamper, proving ownership etc. It is used to verify identity of the owner and thereby create a copyright for the file. There are two steps in watermarking technique called as watermarking embedding and extraction system.

Watermarking can be mainly classified into two types-visible watermarking and invisible watermarking. Visible watermarking refers to information visible on the file. They are embedded logos mostly. For example in an online magazine, the logo of the magazine is seen at an end. Invisible watermarking makes information embed as a digital data. It is mostly used everywhere and can be retrieved quite easily.

2.2 Applications:

- Used for copyright protection
- Used for tracing of source
- Used for annotation of photographs

2.3 Requirements:

- Any type of piracy attack should not affect the embedded watermark
- Should be possessing high level of readability and should be statistically undetectable
- Original multimedia matter should not be lost at any cost
- Both visible and invisible types should permit for accessibility
- Should be secure against forgery and other illegal threats

2.4 Types of water marking

2.4.1 Spatial domain algorithm for gray scale images watermarking

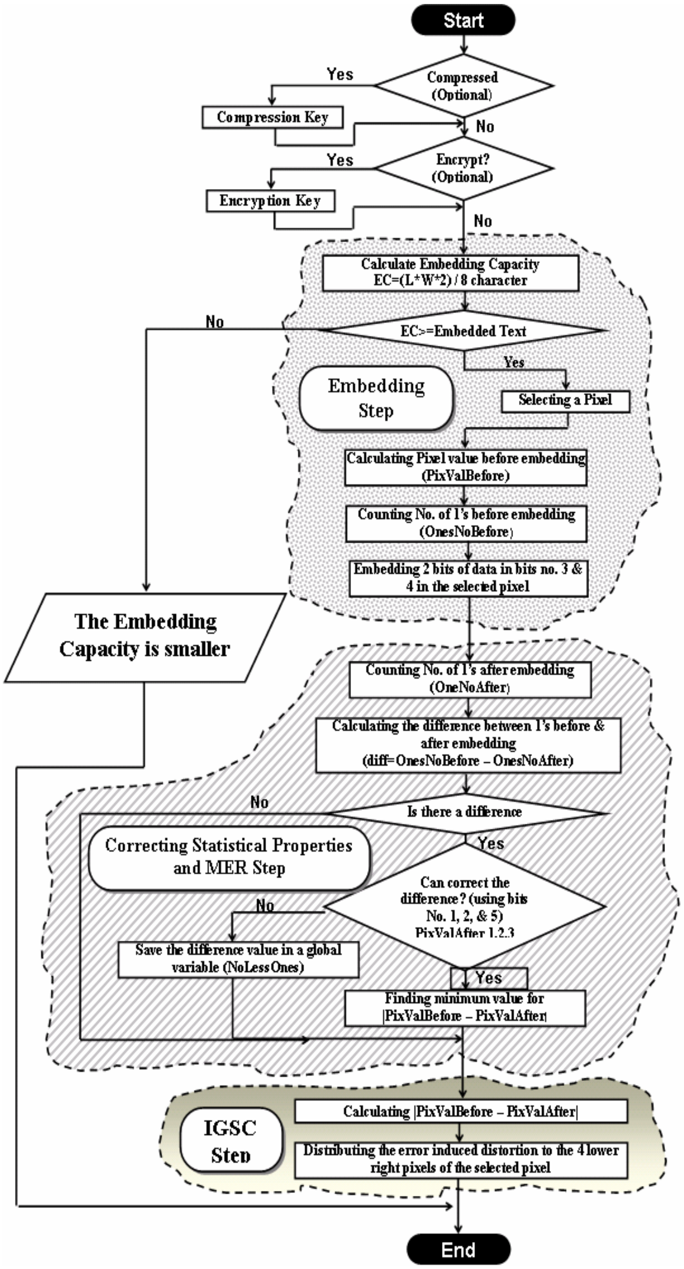

Start
Compressed
(Optional)
Yes
Compression Key
No
Encrypt?
(Optional)
Yes
Encryption Key
No
Calculate Embedding Capacity
EC=(L*W*2) / 8 character
EC>=Embedded Text
No
Yes
Embedding
Step
Selecting a Pixel
Calculating Pixel value before embedding
(PixValBefore)
Counting No. of 1's before embedding
(OnesNoBefore)
Embedding 2 bits of data in bits no. 3 &
4 in the selected pixel
The Embedding
Capacity is smaller
Counting No. of 1's after embedding
(OneNoAfter)
Calculating the difference between 1's before &
after embedding
(diff=OnesNoBefore – OnesNoAfter)
Is there a difference
No
Yes
Correcting Statistical Properties
and MER Step
Can correct the
difference? (using bits
No. 1, 2, & 5)
PixValAfter 1.2.3
No
Save the difference value in a global
variable (NoLessOnes)
Yes
Finding minimum value for
|PixValBefore – PixValAfter|
IGSC
Step
Calculating |PixValBefore – PixValAfter|
Distributing the error induced distortion to the 4 lower
right pixels of the selected pixel
End

Figure 1: Spatial domain algorithm

In this method, watermark is directly embedded in pixels of host image by interchanging the lower order bits of pixels with that of the watermark. Spatial domain technique has relatively low calculation complexity. Spatial technique does not cause any change in the image quality. Least Significant Bit or LSB method is the simplest form of spatial methods. Save algorithm saves some position from host image matrix as a key for watermark extraction. This algorithm is composed of two processes, embedding process and extraction process[2].

2.4.2 Novel multiple spatial watermarking technology in clear images

In this method the host image is fragmented into four regions. Each region has four 128*128 blocks in order to hide a watermark. Watermark is binary image encrypted and embedded into the blue components of the host image. Five watermarks can be extracted by comparing the intensities of the selected region of the original image with the watermarked image.

2.4.2.1 Watermark embedding

Since blue color is more sensitive to human eye, it is chosen to hide the watermarks. Watermark is embedded four times to protect it.

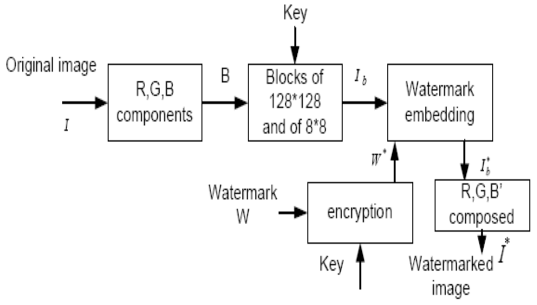


Figure 2: Embedding watermark

2.4.2.2 Watermark detection

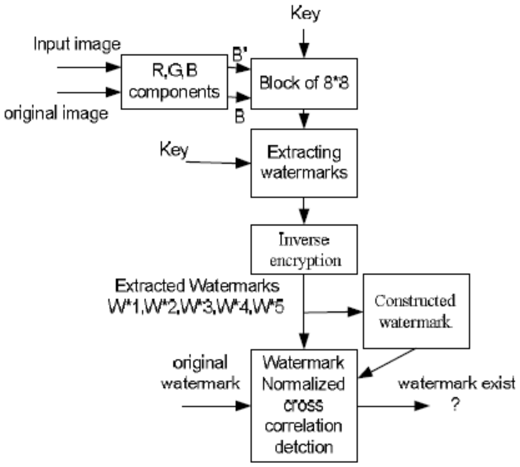


Figure 3: Extraction of watermark

Original image and original watermark are required. First of all the original image and input image are decomposed into regions of 128*128. Five watermarks are extracted by comparing the intensity pixel values of each region in the original image with the watermarked image[5].

2.4.3 A DCT domain visible watermarking technique for images

As already discussed previously digital watermarking is defined as a process of embedding data into a multimedia object to help to protect the owner’s right to that object. From the two available types (that is visible and invisible),choose visible type here in this method. It modifies the DCT coefficients of the host image. The scaling and embedding factors’ values are found out using a mathematical model developed by exploiting the texture sensitivity of the human visual system (HVS). Thus perceptual quality is better preserved.

2.4.3.1 Finding the scaling and embedding factors

For finding the scaling and embedding factors the following steps should be taken into consideration.

They are-

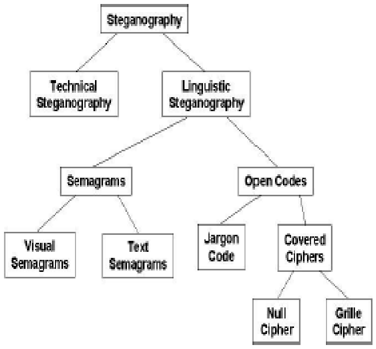
- The edge blocks should be smallest amount altered to evade significant distortion of the image
- Scaling factor alpha should be kept maximum and beta should be kept minimum
- The distortion visibility is little when the background has tough texture
- AC DCT coefficients of greatly textured blocks have small variances and can be inserted more to those blocks.

2.4.3.2 Insertion of watermark

Steps for watermark inclusion are discussed below-

- The original figure and watermarked image are separated into blocks of size 8x8
- The DCT coefficients of each blocks of original image are found out
- For each block of original image, the normalized mean gray value is computed and are scaled
- Normalized image mean gray value is found out
- For AC DCT coefficients normalized variances are computed and scaled
- Edge blocks are identified using Sobel edge operator
- Alpha and beta values are found out
- DCT of watermark images are found out
- nth block DCT coefficient of host image is modified.
- IDCT of modified coefficients grant the watermarked image

2.4.3.3



Modifications to make the watermark more robust

For images having very few objects and large uniform areas. Most of the blocks will be classified to be in one class for this type of image.

The different alpha and beta values are sorted and displayed here to get a clear understanding of the situation. Thus it becomes easier for a thief to remove the water mark as it would be easy to predict alpha and beta values. To evade such a situation a modification is proposed to the insertion technique. It is described as follows-

- If more than 1/3rd of the blocks have the same value, then generate Gaussian random numbers with mean same as the normalized image mean and variance 1.
- Then the numbers are added to normalized beta of the largest group

2.4.4 Collusion attack resistant watermarking scheme for colored images using DCT

Image watermarking with both insensitive detection and high toughness capabilities is still a challenging problem for copyright protection now. Here it deals with a new scheme for hiding a logo based watermark in colored still image which is naturally collusion attack resistant. It is based on averaging of middle frequency coefficients of block discrete cosine transform (DCT) coefficients of that representation.

The main motivation behind selecting middle-band coefficients exchange scheme as a base is that this scheme has proven its robustness against those attacks which any how do not affect the perceptual quality of an image such as JPEG compression[4].

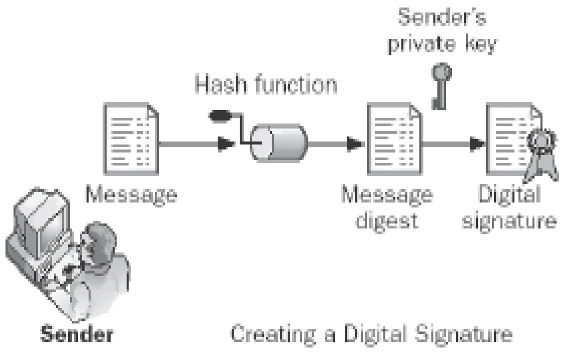
2.4.5 Robust digital image watermarking scheme in DCT domain using fuzzy interference system and human interference system

Fuzzy logic techniques are used to improve the robustness of the watermark, in which they are based on membership values between input and output. Fuzzy logic approach is a process inhibited by human operator. The theory of fuzzy logic tends human approach in the sense that variables are treated not as logical but as linguistic. They do not use mathematical modeling concepts[3].

3. Steganography:

Figure 4 : Steganography

Steganography is the art and science of writing hidden messages where only the sender and receiver can find the existence of the image. It is a method of securing the messages[1].



Techniques of steganography

- Digital
- Network
- Printed
- Digital text etc.

4. Fingerprinting

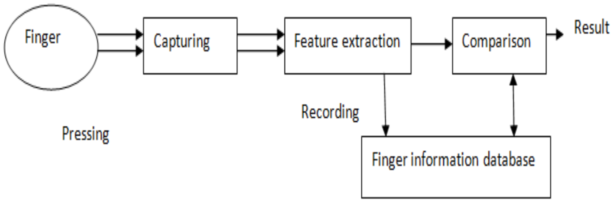


figure 5: Fingerprinting process

Fingerprinting deals with taking each copy of the content and making it unique one to the receiving person. By this way, the exact person who spreads the work initially can be found out.

5. Cryptography

Figure 6 : Cryptography

Cryptography is the practice and learning of techniques for secure communication in the presence of third parties.

Mainly divided into two:-

- Public key cryptography (asymmetric cryptography)Symmetric cryptography.

- Public key cryptography requires two distinct keys-one of which is secret and other is public.
- Symmetric cryptography relies on the same key to perform both.

6. Digital Signature

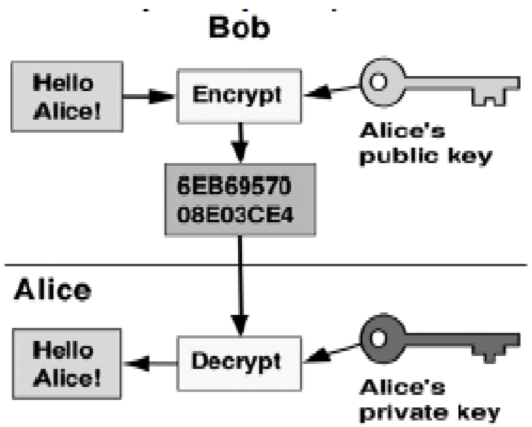


figure 7: Digital signature

It is a mathematical scheme for demonstrating the authenticity of a digital message or document. It consists of three algorithms:-

- Key generation algorithm
- Signing algorithm
- Signature verifying algorithm

7. Conclusion

Since digital information such as images and videos are dominant in internet data hiding techniques are necessary. Many methods can be used for data hiding. Digital watermarking is the more secure method.

8. References

1. Digital watermarking and other data hiding techniques International journal of innovative technology and exploring engineering(IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April-2013

2. A new spatial domain algorithm for gray scale images watermarking Proceedings of the international conference on computer and communication engineering 2008, May 13-15, 2008, kuala lumpur, Malaysia

3. A new lossless watermarking scheme based on fuzzy integral and DCT domain 2010 international conference on electronics and information engineering

4. An improved Digital watermarking technique for protecting JPEG images West virginia university Morgantown, WV, USA

5. A Bioorthogonal wavelet transform based on robust watermarking scheme 2012 IEEE conference on Electical, Electronics and Computer Science

Dr.K.SATHIYASEKAR, obtained his Ph.D. Degree in High Voltage Engineering, from Anna University, Chennai. He has a total teaching experience of 22 years in various Institutions at B.E and M.E levels. He has published / presented 35 research papers in International Journals / Conferences, and has received the **Best Paper Award** for his paper titled "Application of BPN Algorithm for Evaluating Insulation Behavior of High Voltage Rotating Machines" in the International Conference on Digital Factory 2008, held at Coimbatore Institute of Technology. He was **awarded travel grant by the Department of Science and Technology, Government of India**, to present his research paper in the **International Conference INDUCTICA - 2010, at Messe Berlin, Germany**, in 2010.

S.Karthick, obtained his Master Degree in Applied Electronics, from Anna University, Chennai. He has 7 years of teaching experience and 6 years in industries. He has presented 14 research papers in International / national Conference. His main area of research is image processing.

Swathy Krishna K.S, she is pursuing M.E in The Kavery Engineering College. She completed her Bachelor degree from Matha College of Technology affiliated to Mahatma Gandhi university.