International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7579-7583
© Research India Publications. http://www.ripublication.com

Digital Watermarking Using Matlab

B.Uma Surya Sai
Student, Department of Electronics and Communication Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India.

R.Samyukta
Student, Department of Electronics and Communication Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India.

P Vandana
Student, Department of Electronics and Communication Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India.

K.Surekha
Student, Department of Electronics and Communication Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India.

A.V.Paramkusam
Professor, Department of Electronics and Communication Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, India.
Orcid Id: 0000-0001-5652-9550

Abstract

Digital watermarking is the act of hiding message related to a digital signal (i.e. an image, audio, and video) within the signal itself. Nowadays, digital water marking has many applications such as broadcast monitoring, owner identification, proof if ownership, transaction tracking, content authentication, copy control, device control and file reconstruction. This watermarking technique is used instead of steganography and cryptography. Here in this technique we used a text type of message which is embedded into an image using some kind encoding key to prevent eavesdroppers to decode the message if the message was intercepted during transmission. Then the message would be transmitted on a communication channel, which would add some noise to the encoded message. The main specification of watermarking is: Robustness, Imperceptibility, and capacity.

Keywords: watermarking, intercept, eavesdroppers, robustness, imperceptibility.

INTRODUCTION

Embedding a hidden stream of bits in a file is called Digital Watermarking. The file could be an image, audio, video or text. The term "Digital Watermark" was coined by Andrew Tirkel and Charles Osborne in December 1992. The first successful embedding and extraction of a stenographic spread spectrum watermark was demonstrated in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin.

Watermarks are identification marks produced during the paper making process. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They were used as a means to identify the papermaker or the trade guild that manufactured the paper. The marks often were created by a wire sewn onto the paper mold. Watermarks continue to be used today as manufacturer's marks and to prevent forgery.

Due to the increasing popularity and accessibility of digital manipulation and copying hardware and software, malicious tampering and illegal reproduction of multimedia information has become difficult to detect. Digital rights management (DRM) has been an active area of research for the past decade, aiming to stop theft and tampering of digital media content. DRM was chosen as one of the top ten emerging technologies that would “change the world”.

The goal of DRM is to detect, track and possibly prevent unauthorized manipulations and distribution of intellectual property. Digital watermarking is one of the components of DRM that can be used to provide evidence of ownership and

tampering. Digital watermarking has already been implemented in various products; however, its success is limited due to limited effectiveness and lack of legal support. This thesis examines digital watermarking from application oriented perspectives. Our aim is to advance the technology and propose cost efficient schemes to advance its use in protecting intellectual property and privacy.

EXISTING METHODS

Steganography and cryptography are the few of the existing techniques for secure communication in the presence of third parties called adversaries.

Steganography is changing the image in a way that only the sender and the intended recipient is able to detect the message sent through it. It is invisible, and thus the detection is not easy. It is a better way of sending secret messages than encoded messages or cryptography as it does not attract attention to itself.

There are many ways in which steganography is done. The messages appear as articles, images, lists, or sometimes invisible ink is used to write between the lines. Steganography is achieved by concealing the information in computer files. Sometimes steganographic codes are inside the transport layer like an image file, document file, media files, etc. Due to the large size of the media files, they are considered ideal for steganography.

Cryptography is the science of writing in secret code and is an ancient art[14] .Cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.Modern cryptography is heavily based on mathematical theory and computer science practice. Drawbacks of cryptography
are

Encryption Keys: If you lose the key to the encryption, you have lost the data associated with it.

Expense: Data encryption is expensive

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal.[2] Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

PROPOSED METHODOLOGY

To overcome the drawbacks of existing techniques we implement watermarking technique. Watermarking is used to verify the identity and authenticity of the owner of a digital image. It is a process in which the information which verifies the owner is embedded into the digital image or signal. These signals could be either videos or pictures or audios. For example, famous artists watermark their pictures and images. If somebody tries to copy the image, the watermark is copied along with the image.

Watermarking is of two types; visible watermarking and invisible watermarking.

Visible Watermarking:

As the name suggests, visible watermarking refers to the information visible on the image or video or picture. Visible watermarks are typically logos or text. For example, in a TV broadcast, the logo of the broadcaster is visible at the right side of the screen.

Invisible Watermarking:

Invisible watermarking refers to adding information in a video or picture or audio as digital data. It is not visible or perceivable, but it can be detected by different means. It may also be a form or type of steganography and is used for widespread use. It can be retrieved easily.

In this project, we will introduce how to use MATLAB to implement image watermarking algorithms. These algorithms include the most famous ones which are widely used in current literature or more complicated approaches are based upon. These are commonly divided into three categories (Barni & Bartolini, 2004)

1. Watermarking in Spatial Domain

2. Watermarking in Spectral Domain

3. Watermarking in Hybrid Domain

The supported formats by MATLAB are: bmp, cur, fts(fits), gif, hdf, ico, j2c(j2k), jp2, jpf(jpx), jpg(jpeg), pbm, pcx, pgm, png, pnm, ppm, ras, tif(tiff), and xwd. ‘A’ is now a matrix of pixels brightness values. If the image is in black and white, the matrix is 2-dimmensional.

However, if there is a color image, we will have a 3-dimmensional matrix, which has three planes of main colors: Red, Green, and Blue. The number of bits that are needed to preserve the value of every pixel is called “bit depth” of the image. The output class of “imread” command is “logical” for

depth of one bit, "uint8" for bit depth between 2-8, and "uint16" for higher bit depths.

Here in text watermarking we use spatial domain algorithm. The text to be watermarked is converted into into their respective ASCII codes and then to binary and inserted in the image.

Watermarking in spatial domain:

The message can be any coded or straight arrange of bits. The command "bitget" can be used here to create the bit-plane splitter function as depicted below:

```
function [B8,B7,B6,B5,B4,B3,B2,B1] = bitplane (pic)
B1 = bitget(pic,1)*2^0;
B2 = bitget(pic,2)*2^1 ;
B3 = bitget(pic,3)*2^2 ;
B4 = bitget(pic,4)*2^3 ;
B5 = bitget(pic,5)*2^4 ;
B6 = bitget(pic,6)*2^5 ;
B7 = bitget(pic,7)*2^6 ;
B8 = bitget(pic,8)*2^7 ;
End
```

The first bit-plane is the least significant one (LSB) and most of the time is hardly related to the main shapes of the picture.

Evaluation of watermarking methods:

Several Functions are used to qualify the watermarking algorithm, examining tests on the resulted watermarked image.

MSE

Mean Squared Error (MSE) is one of the earliest tests that were performed to test if two

pictures are similar. A function could be simply written according to equation.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(X_i - X_i^*\right)^2$$

```
function out = MSE (pic1, pic2)
e=0;
[m,n]=size(pic1);
for i=1:m
for j=1:n
e = e + double((pic1(i,j)-pic2(i,j))^2);
end
end
out = e / (m*n);
end
```

PSNR

Pick Signal to Noise Ratio (PSNR) is a better test since it takes the signal strength into

consideration (not only the error). Equation (4) describes how this value is obtained.

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

```
function out=PSNR(pic1, pic2)
e=MSE(pic1, pic2);
m=max(max(pic1));
out=10*log(double(m)^2/e);
end
```

Noise attack

Adding noise in MATLAB is simply done by "imnoise" command. Gaussian, Poisson, Salt &

Pepper, and Speckle are among the noises that could be used here. Fig. 14 shows the result

of the code:

```
Lena = imread('lena.tif');
Lena = imnoise(Lena,'salt & pepper',0.02);
imshow(Lena);
```

Figure 1: Salt & Pepper noise

RESULTS

when the image is subjected to text water marking the binary values of the message are inserted at some position of the image based on the code. Due to this insertion, the value of pixel may be increased, so slight change is observed. The image in fig (2) is before watermarking and its pixel.

Figure 2: Before watermarking

The corresponding pixel values of original image i.e.; for only for some part of image.

a <512x512 uint8>

	1	2	3	4	5	6	7	8	9
1	161	162	163	162	163	156	162	162	165
2	162	162	162	161	163	156	162	162	166
3	163	163	162	160	163	157	163	162	167
4	163	163	162	160	162	158	164	162	167
5	163	163	161	159	162	158	164	161	164
6	162	162	160	158	162	158	163	159	161
7	160	161	159	156	161	158	162	156	159
8	159	159	158	155	160	157	161	154	159
9	155	156	157	157	158	159	159	159	161
10	155	156	157	158	158	157	155	155	162
11	156	155	157	159	158	154	152	151	160
12	157	155	157	159	158	154	151	152	160
13	157	156	156	158	158	155	154	155	162
14	157	157	157	157	157	157	157	157	158
15	157	159	158	156	156	158	158	156	156
16	156	160	160	156	155	158	157	154	159
17	157	155	155	157	157	155	154	154	157
18	157	156	156	157	157	155	153	153	157
19	157	156	156	157	157	156	154	154	158
20	155	155	156	157	157	157	156	156	160
21	155	155	156	156	156	157	157	157	160
22	156	157	157	155	155	155	156	156	158

When the original image is watermarked with a text then the following results are observed.

The corresponding pixel values are:

wm <512x512 uint8>

	1	2	3	4	5	6	7	8	9
1	209	211	211	210	211	204	210	162	165
2	211	211	210	209	210	204	210	162	166
3	211	211	210	208	211	204	211	162	167
4	210	211	210	208	210	206	212	162	167
5	211	211	209	206	211	206	212	161	164
6	211	211	208	207	210	206	211	159	161
7	209	209	206	205	209	206	210	156	159
8	207	207	207	202	209	204	208	154	159
9	203	205	204	205	207	206	206	159	161
10	203	205	204	206	207	204	203	155	162
11	204	203	204	206	206	202	200	151	160
12	205	203	204	207	207	203	199	152	160
13	205	205	204	206	207	203	202	155	162
14	204	205	204	204	204	204	204	157	158
15	205	207	207	204	205	206	206	156	156
16	205	209	208	205	202	206	204	154	159
17	205	203	202	204	205	202	203	154	157
18	204	205	204	204	204	202	200	153	157
19	205	205	205	204	204	204	202	154	158
20	203	203	205	204	204	205	204	156	160
21	203	203	204	205	205	205	205	157	160
22	205	205	204	203	202	203	204	156	158
23	205	207	204	202	201	202	205	156	157
24	205	205	204	200	200	203	205	158	158
25	205	207	205	200	201	204	206	159	160

Therefore, by implementing text watermarking any text message can be embedded into an image and some properties can be inculcated like

Robustness: The watermark should be able to withstand after normal signal processing operations such as image cropping, transformation, compression etc. Robust watermarks may be used in copy protection applications to carry copy and no access control information. A digital watermark is called *semi-fragile* if it resists benign transformations, but fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformation.

Imperceptibility: The watermarked image should look like same as the original image to the normal eye. The viewer cannot detect that watermark is embedded in it.

Security: An unauthorized person cannot detect, retrieve or modify the embedded watermark.

CONCLUSION

The implementation of basic digital watermarking methods in MATLAB is described. Fundamental methods in spatial, spectral, and hybrid domains are described and sample codes are given. Finally, some solutions for qualifying the watermarking method are described.

FUTURE SCOPE AND APPLICATIONS

This thesis work can be extended in two main areas. First, each proposed technique can be improved to better address the applications they are intended for. Furthermore, the digital watermarking techniques can be developed to provide better protection for the intellectual property.

Digital watermarking may be used for a wide range of applications, such as:

- Copyright protection
- Source tracking (different recipients get differently watermarked content)
- Broadcast monitoring (television news often contains watermarked video from international agencies)
- Video authentication

REFERENCES

[1] Ingemar J. Cox: *Digital watermarking and steganography*. Morgan Kaufmann, Burlington, MA, USA, 2008

[2] Frank Y. Shih: *Digital watermarking and steganography: fundamentals and techniques*. Taylor & Francis, Boca Raton, FL, USA, 2008.

[3] A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. "Electronic Water Mark". DICTA 93, Macquarie University. p.666-673

[4] Khan, A. and Mirza, A. M. 2007. Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding. *Inf. Fusion* 8, 4 (Oct. 2007), 354-365

[5] Copy Protection Technical Working Group (CPTWG)

[6] *Paul Blythe; Jessica Fridrich,* Secure Digital Camera *(PDF)*

[7] Saraju Mohanty, *Nagarajan Ranganathan, and Ravi K. Namballa,* VLSI Implementation of Visible Watermarking for a Secure Digital Still Camera Design *(PDF)*

[8] Vatsa, M.; Singh, R.; Noore, A.; Houck M. M. & Morris K. (2006). Robust biometric image watermarking fingerprint and face template protection. *IEICE Electronics Express, Vol. 3, No. 2, pp. 23-28*

[9] Wang, Z.; Bovik, A. C.; Sheikh, H. R. & Simoncelli E. P. (2004).Image quality assessment: From error visibility to structural similarity. *IEEE Trans. Image Processing*, vol. 13, no. 4, pp. 600-612.