A Modification of Least Significant Digit (LSD) Digital Watermark Technique

Naseem Masoud Asad Princes Alia University Collage Al-Balqa Applied University Amman-Jordan

ABSTRACT

This study presents the modification of the Least Significant Digit (LSD) Digital Watermark Technique based on optimizing the selection pixels in cover image. Specific pixel's value in cover image will modified in not randomly way. Random selection of pixel's value will not achieve the accurate reliability. Optimizing selection reduces the number of pixel's value which will modified. In this study the Least Significant Digit (LSD) Digital Watermark Technique and The process of optimizing selection are applied. The digital watermark and digital cover image is in gray scale. The processing domain is in spatial domain.

Keywords

Watermarking, Steganography, Embedding, Extracting, Pixels

1. INTRODUCTION

Information hiding is a general term that include covert channels, anonymity, steganography, and watermarking.[1]

Watermarking is a technique used to embed data or identifying information within digital multimedia such as digital image. Our discussion will focus primarily on the optimization selection of pixels value in digital cover image of grayscale which corresponds to watermark. Digital binary image (watermark) will be embedded in cover image. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information.

The digital watermarking process embed data such as copyright or fingerprinting into the media without significantly degrading its visual quality. Recently digital watermarking technique is used to embed specific information, such as author information called watermark into different kinds of media called Cover Work [2, 3].

Steganography is a term derived from the Greek words steganos, which means "covered or hidden" and graphia, which means "writing" [4].

Steganography is a technique for information hiding. it is the art and science of invisible communication of messages It aims to embed invisible data into a digital cover media, such as digital audio, image, video, etc. We can use digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information as covers or carriers to hide secret messages. After embedding a secret message into the cover image, we obtain a so-called stego image. It's important that the stego image doesn't contain any detectable artifacts due to message embedding.[5]

Both techniques embed a message m in some cover data d, to obtain d', practically indistinguishable from d [6], as shown in figure 1.

Ismail Ghazi Shayeb Princes Alia University Collage Al-Balqa Applied University Amman-Jordan



Fig 1: Embedding process in steganography and watermarking

However, they have different goals and requirements as shown in table 1.[7]

Fable 1. The difference between Steganography	and
watermarking	

Steganography	Watermarking
Breganography	Water him hing
An eavesdropper must not be able to detect the presence of m in d'	An eavesdropper cannot remove or replace m in d'
Primarily for 1-to-1	Primarily for 1-to-many
communication	communication
Robustness not typically an	Robustness of watermark is a
issue	main issue
Capacity desired for message	Known watermark may be
is large	there
Always invisible	Can be visible or invisible
Typically dependent on file format	Watermark can be considered to be an extended data attribute

MATERIALS AND METHODS Least Significant Digit (LSD) Digital

Watermark Technique

This technique used to embed digital watermark in digital image based on random selection of pixel's value to be modified.

2.2 Embedding Process

First of all, some processes on the watermark and cover image must implemented. The watermark image will be converted to binary image as shown in Figure 2. While the cover image will converted to grayscale image as shown in figure 3.



Fig 2: Watermark



Fig 3: Cover Image, "Lena" image

Modification pixels value of digital cover image which corresponds to text pixels to have a specific (2, 3, 7 and 8) digits as (LSD), as shown in Figure 4. Also modification all pixels values have (2, 3, 7 or 8) (LSD) which is not correspond to text pixels is necessary; otherwise some black area may appear around the text after extracting process.

210	214	214	214	214	214	210	210	214	216	210	214	214
210	210	210	210	210	216	210	210	219	214	216	210	216
210	212	213	212	210	217	210	213	219	217	216	210	216
214	210	213	210	210	217	210	212	219	217	216	210	216
210	214	213	210	210	218	213	213	219	217	216	210	214
210	214	212	214	214	218	214	212	219	218	214	210	214
210	216	208	216	214	218	219	217	216	218	217	218	214
210	210	210	216	210	214	219	219	210	210	214	210	214

Fig 4: Modifying pixels values that have (2, 3, 7 and 8) LSD

2.3 Extracting Process

Appearing the pixels which have (2, 3, 7 or 8) LSD to get the embedded text and the final result will give only the text clearly without unexpected area.

3. MODIFICATION OF THE PREVIOUS TECHNIQUE

This modified technique based on frequents least significant digit of pixels value to optimize the selection. It is an important to make a pre-calculations or statistics on cover image pixel's value to optimize the selection of pixel's value which will be modified. The following steps explain the optimization selection:

Step 1: Finding the frequent of each least significant digit of each pixel's value in cover image as shown in Table (2).

Table 2:An example of frequents pixel's values in cover image (800x600)

LSD value	Frequent
9	46000
8	60000
7	42000
6	37000
5	53000
4	39000

3	56000
2	57000
1	35000
0	55000

Step 2: Arranging the table data in Table1 descending depending on frequent column as shown in Table (3).

Table 3: Table (2) after ar	ranging
-----------------------------	---------

LSD value	Frequent
8	60000
2	57000
3	56000
0	55000
5	53000
9	46000
7	42000
4	39000
6	37000
1	35000

Step 3: Selecting the last LSD pixel's values in Table (3) to be the LSD which will modified in the cover image.

So, the number of selecting pixel's with LSD values (1,6,4,7 and 9) is the minimum number of pixel's values which will modified.

4. RESULT AND DISCUSSION

It is more reliability to reduce the number of pixel's values which will modified within cover image during embedding process.

This optimization guaranteed that the minimum numbers of pixel's values will changed in cover image, to get the cover image more reliability, as shown in figure 5.



Fig 5: The relation between the reliability and the number of changed pixel's value.

According to the values in Table 3, If the random selection is implemented such as pixel's with (8,5,3,7 and 4) LSD values, then the number of changed pixel`s value=60000+53000+56000+42000+39000=250000 pixel's value. However, if the optimization selection is implemented, then the number of pixel's with(9,7,4,6 and 1) LSD values must selected. So, the number of changed pixel's value=46000+42000+39000+37000+35000=199000 pixel`s value. Depending on previous equations results and figure 5, using the optimization selection achieves more reliability than random selection. Because the optimization selection changed pixel's values less than random selection ie. 199000 < 250000.

Random selection don't achieve the reliability because it may modify a lot of number pixel's values in cover image.

5. CONCLUSION

Reducing the number of pixel's value which would be selected for modification within cover image increases the cover image reliability. The optimization selection achieves more reliability because it used the minimum numbers of pixel's values that changed in cover image.

The ideal solution to achieves the maximum reliability is keeps the pixel's values of the cover image without changing.

This optimization selection keeps the same image size after embedding process.

6. REFERENCES

- [1] Provos Niels, (2009), "Hide and Seek: Introduction to steganography". IEEE Computer society.
- [2] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518.
- [3] B Surekha, Dr GN Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011.
- [4] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt "Digital image steganography: survey and analysis of current methods" Signal processing, Volume 90, Issue 3, March 2010, pp. 727-752.
- [5] S.Shanmuga Priya, K.Mahesh, Dr.K.Kuppusamy/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2632-2637.
- [6] Amaobi Uwaleke Michael, Amadi Emmanuel Chukwudi, Nwokonkwo Obi Chukwuemeka. A Cost Effective Image Steganography Application for Document Security. Management Science and Information Technology. Vol. 2, No. 2, 2017, pp. 6-13. doi: 10.11648/j.msit.20170202.11.
- [7] https://fenix.tecnico.ulisboa.pt/downloadFile/112651838 2176626/csf-22.pdf, P36-37.
- [8]