2016

International Journal of Humanities & Information Technology (IJHIT)

Volume – 1, Issue - 1

ISSN : Applied

INTERNATIONAL JOURNAL OF HUMANITIES & INFORMATION TECHNOLOGY
(IJHIT)

WWW.IJHIT.COM

Fingerprinting and Data Hiding Based on Spread Spectrum

Amit Singh

(Assistant Professor/Department of Computer Science/ SR Group of Institutions/ Lucknow)

Abstract: *The digital information revolution has brought about profound changes in our society and our lives. The many advantages of digital information have also generated new challenges and new opportunities for innovation. This thesis discusses the issues regarding multimedia data hiding and its application to multimedia security and communication, addressing both theoretical and practical aspects, and tackling both design and attack problems.*

Spread-spectrum embedding borrows ideas from spread-spectrum modulation. The basic process of spread-spectrum embedding consists of four steps. The first step is to identify and compute features that will carry watermark signals. Depending on the application and design requirements, the features can be signal samples, transform coefficients (such as DCT and DFT coefficients), or other functions of the media content.

Keywords: *Digital Fingerprint , Watermarking Signal, DCT and DFT coefficient, JND*

1. Introduction

We generate a watermark signal and tune its strength to ensure imperceptibility. Typically, we construct the watermark to cover a broad spectrum as well as a large region of the content, resulting in a watermark that resembles noise. A third step is to add the watermark to the feature signal. Finally, we replace the original feature signal with the watermarked version and convert it back to the signal domain to obtain a watermarked signal. The detection process for spread-spectrum watermarks begins with extracting features from a media signal in question. Then the similarity between the features and a watermark is examined to determine the existence or absence of the watermark in the media signal. Typically, a correlation similarity measure is used, often in conjunction with preprocessing (such as whitening) and normalization. An example of spread-spectrum watermarking for image is provided in Figure 1

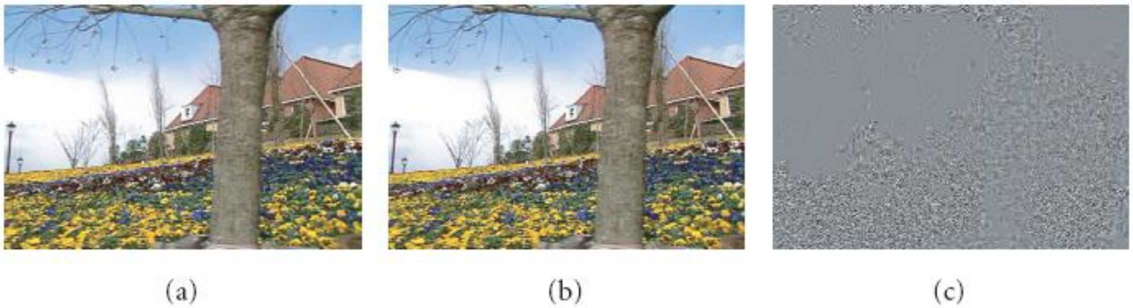


Fig:1: The original flower garden image, the watermarked version, and the watermark embedded, respectively. The watermark shown is the amplified difference between the original and the watermarked versions by a factor of 5, with mid-level gray denoting zero amplitude and black/white denoting large amplitude.

2. Technique:

We use three phase to hide data using spread spectrum

2.1 Phase-1

In our experiment, we have first taken the 2D DCT of the cover image, then these coefficients' have been reshaped to form a single dimensional matrix. Next the watermark is taken, in our case, the logo; the 2D DCT of this watermark is taken and is reshaped to form a single dimension array. It is to be noted that the array size of the cover image will be 1x786432 (768*1024=786432) and the array size of the watermark image will be 1x16384 (128*128).Now in order to do the embedding these DCT coefficients are simply added, but before doing this, the size of the watermark array is made equal to that of the image by adding zeroes to the array. Fig 2 shows how the watermark is inserted in the cover image

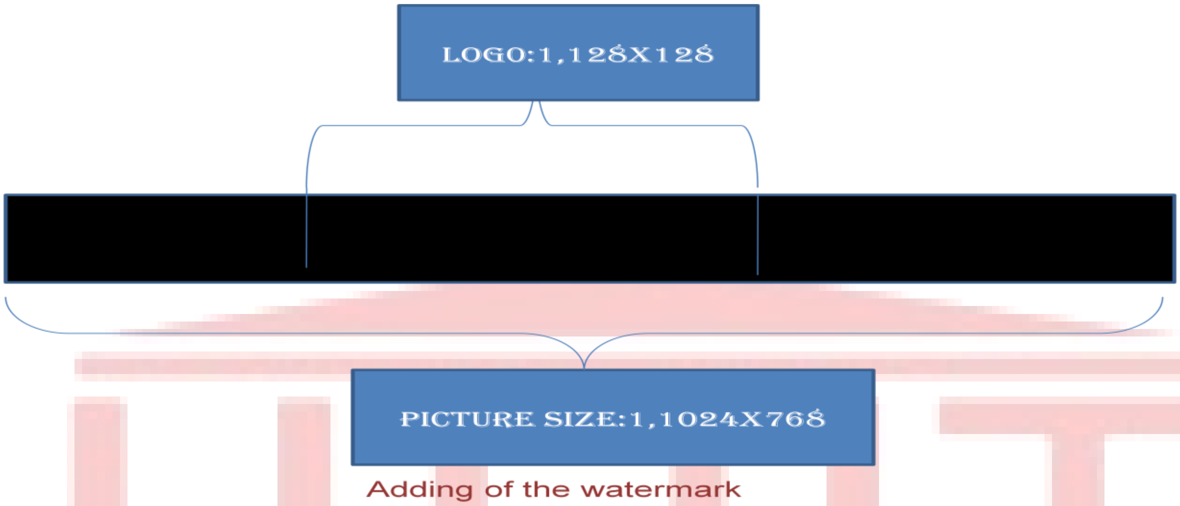


Fig2 : adding of the watermark

2.2 Phase-2

The correlation of the retrieved watermarks is then found out; with respect to the original watermark (random data stream) the average of these co-efficients is then plotted in a graph with respect to the overlap. The overlap percentage is computed according to the given formula:

Ovlp= ((b1+logo_size)-b2)/logo_size

Where,

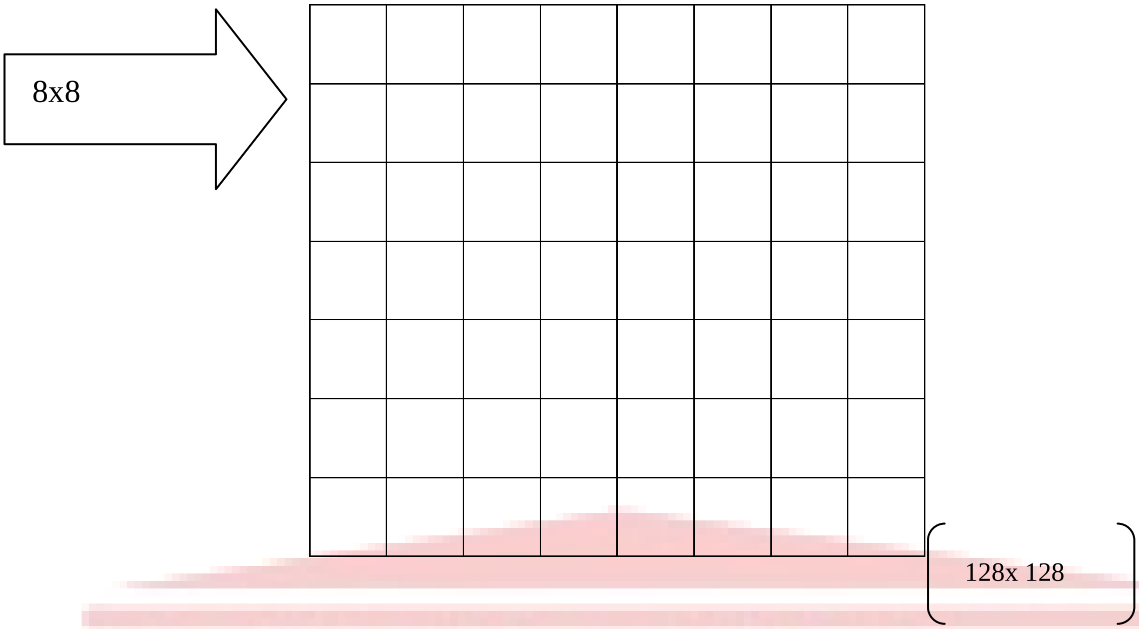
logo_size=size of the random data stream

b1, b2 are the two random starting points where the watermark is inserted

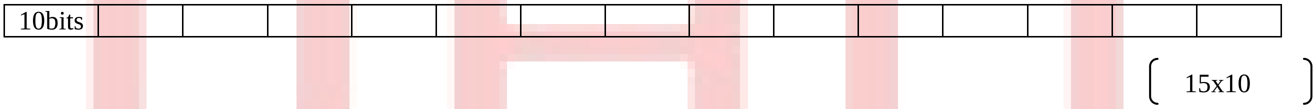
2.3 Phase-3

Fig3. base image of size 128x128.

Shown above is the base image.This image is now divided into much smaller blocks of size 8x8



After diving the image in 8x8 such smaller blocks we obtain a total of 16x16(256) small blocks.The watermark is taken of size 10x15, which is linearised and is divided into 15 blocks each of bit length 10 as shown below:



Now the image blocks are chosen at a random order using the row number and the column number where the watermark is to be inserted, and the 10 bits of that particular image block shown in the figure below is added with the 10 bits of the watermark block.This procees is repeated 15 times for the 15 different blocks in the watermark,sequentially

1	1	1	1	0	0	0	0
1	1	1	0	0	0	0	0
1	1	0	0	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Advantage

There are following advantage of our methodology

a) *it* save our system from ***Subtractive attack, Distortive attack, Additive attack***
b) it is used for two-tier group-oriented fingerprinting.

Result

By taking two argument b1 & b2 we can find out overlapping percentage and correlation coefficient as given below in table and graphical analysis .

b1	b2	overlap%	corr1	corr2
10000	10500	87.79297	0.6615	0.6685
1000	1500	87.79297	0.6698	0.6595
5000	5500	87.79297	0.6764	0.6764
2000	2500	87.79297	0.6598	0.6667
2	502	87.79297	0.6684	0.6583
20000	20500	87.79297	0.658	0.6692
700000	700500	87.79297	0.6631	0.6573
20000	24000	2.34375	0.6974	0.6953
2000	6000	2.34375	0.7005	0.6974
1000	5000	2.34375	0.6944	0.6972
2	4002	2.34375	0.6936	0.7016
5000	9000	2.34375	0.697	0.7004
10000	14000	2.34375	0.6925	0.6957

Table: table showing the overlap percentages and the corr1, corr2

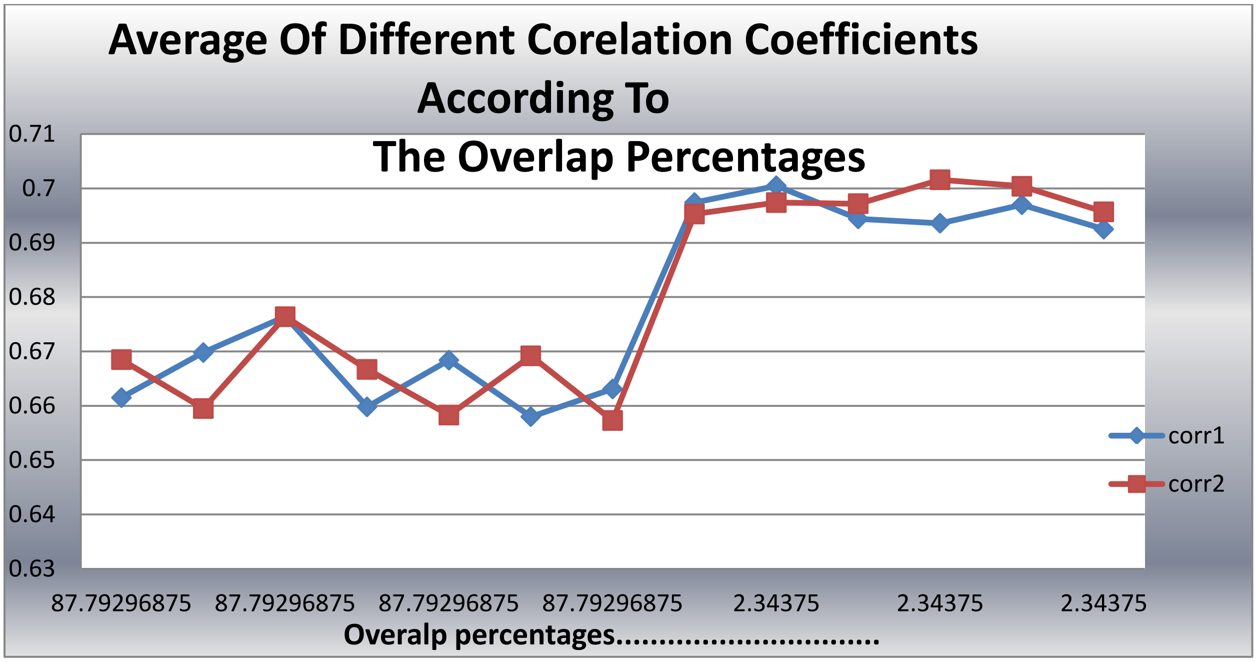


Fig: the overlap percentages against the different correlation coefficients

Conclusion

As it is obvious that the number of combinations is a very huge number, hence it would be almost impossible for an attacker to attack. Moreover we have already established the position independence of the watermark and its robustness against compression and averaging attack. Along with the position independence of the watermark, the watermark block can also be chosen randomly.

Thus we can conclude that the watermarking technique employed is a very sturdy and robust one

REFERENCES

[1]. I. J. Cox, J. Bloom, andM.Miller, *DigitalWatermarking: Principles& Practices*, Morgan Kaufmann Publishers, San Francisco,Calif, USA, 2001.

[2]. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[3]. R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108–1126, 1999.

[4]. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[5]. M. D. Swanson,M. Kobayashi, and A.H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, 1998.