International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

EMBEDDING WATERMARK INTO AN IMAGE USING SEQUENCES

AMITOZ SINGH RATHORE[1], SUR SINGH RAWAT[2]
[1,2]Department Of CSE
JSSATE Noida

Article Received: 07/03/2015 | Article Revised on14 /03/2015 | Article Accepted on:18/03/2015

Amitoz Singh Rathore

ABSTRACT

Innovation of technology and having fast internet makes information to be distributed over the worldeasy and economical. This has made people to worry about their privacy and works so we present a techniquethat prevents unauthorized users to have access to the important data. Steganography and digital watermarkingprovide methods so that users can hide and mix their information within other information that make it difficult torecognize by attackers. In this paper, wepresent a technique of embedding watermark using sequences into an image.

Keywords: -Watermark,Sequence,Key, Secret

I. INTRODUCTION

The aim to communicate secretly is as old as communication itself. Internet has become an important part of the infrastructure of today's world. The information to be transferred comes in different forms and is used in different applications. Defense communication systems make good use of security methods which, rather than not only concealing the content of a data using encryption, aim to conceal its sender, its receiver or its presence. Similar methods are applied in some cellular phone systems and methods of digital elections. Hackers aim to use whatever safety properties are provided intentionally or otherwise in the available communications systems and police forces try to restrict their use.

A large focus of information security has always been on cryptography. The idea behind cryptography is to change (that is, encrypt) the source material such that it becomes impossible to correctly interpret, outside of the intended senders and recipients. A much less common method of security, called steganography, has been a growing area of focus amongst the digital community. Steganography is the art of communicating in a way which hides a secret message in the main information. Steganography seeks to encode information. From steganography a technique of authorization is evolved called watermarking, is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted to make an assertion about the object. A watermark can be perceived as an attribute of the carrier (cover). It may contain information such as copyright, license, tracking and authorship etc. Its use is as old as paper

manufacturing. Paper Watermarks have been in wide use since the late middle ages. Their earliest use seems to have been to record the manufacturer's trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock.

II. Proposed method

One of the techniques of embedding data in the cover image is the Lsb technique. In Lsb technique the data is embedded into the last bit so that it cannot be detected by human eye.At the sender end data is embedded and then data is extracted at the receiver end. This method has the drawback as the location of the embedded data bits can be easily known as data is embedded sequentially and data can be altered. So our data will be lost. To overcome this problem we need to insert data not sequentially but in a random way at random indexes and instead of embedding data at the last bit second last and third last bit can be used to insert data. We can embed data in the image at random indexes at the sender end and extract at the receiver end.

Embedding Procedure at sender End:-

Input: Cover Image, Watermark Image ortext, seed
Output: Watermarked Cover Image
Begin:
Select the cover image in which watermarking is to be done.
Input seed to generate random sequence.
Generate the random sequence of indexes at which embedding is to be done.
Select the option whether to enter watermark as text or watermark as image.
If watermark is text convert the ascii code into bits.
Embed the watermark bits in the cover image at the indexes generated randomly.
If the watermark is image.
Check the dimension of the watermark image.
If dimension of watermark image is more
than cover image reject the watermark image.
Embed the watermark bits in the cover
image at the indexes generated randomly .
Generate Key From the Watermark Image.
Display the watermarked Image
End

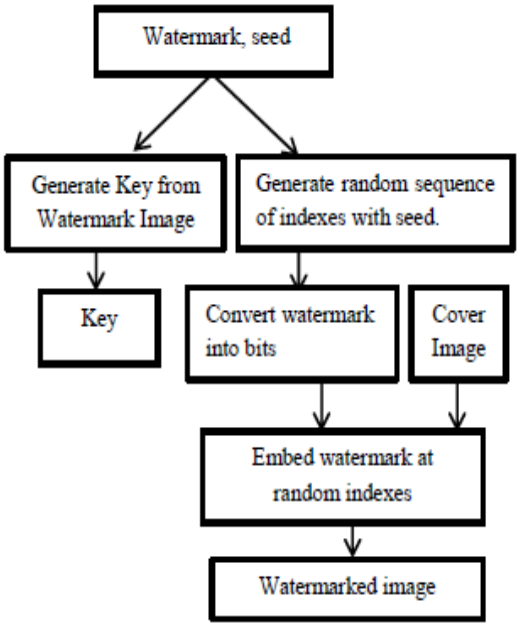

Fig.1 Embedding procedure at sender end

Key generation: -Let the key to be generated by the watermark image be K .Consider the watermark to be an m x n image. The elements in the image are read as a m × n matrix. For example, consider the following 9 × 12 image to be the watermark.

Fig.2.1Watermark

Image read in form of matrix

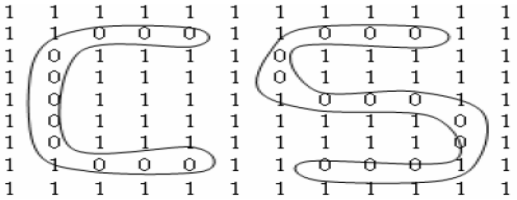

Fig.2.2. Digital sequence of watermark

The image is read in the form of a matrix as the elements of the matrix are rearranged into a single array so that the size of the matrix is 1× (m×n), that is, 1×108 as shown below.

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

Now these elements are split into bits of 't' each. The number sequence so that the total number of

elements are divisible by 't'. For that, the number sequence is appended by 0 s, if needed, to reach the limit that the total number are divisible by 't'.If the value of 't' is taken to be 5, then the above sequence can be split as

1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 1 1 1 0 1 1 1 1 1
31 31 16 14 31
0 1 1 0 1 1 1 1 1 0 1 1 0 1 1 1 1 0 1 1 1 0 1 1 1 1 1
13 30 27 29 31
1 1 1 1 1 1 0 0 1 1 1 1 1 0 1 1 0 1 1 0 1 1 0 1 0 1
31 19 30 27 13
1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 0 1 1 1 1 1 0 0 1 1 1
22 27 13 31 7
1 1 1 1 1 1 1 1 0 0
31 28

The obtained array is used as the key for embedding noise into the image.

K (key) = 31 31 16 14 31 13 30 27 29 31 31 19 30 27 13 22 27 13 31 7 31 28

Recovery procedure at receiver end:

Input : Watermarked image
Output: Extracted watermark as text or image.
Begin:
Generate the random sequence of indexes with the seed at which embedding was done
Input whether embedded watermark is image or text.
If embedded watermark is text
Extract the text bits from the watermarkedimage.
Convert the bits into ascii code.
Display the watermark text.
If the embedded watermark is image
Generate the watermark image using the key.
Extract the watermark image as bits fromcover image.
Watermark as bits is Extracted
Convert the bits into the Watermark image .
Display the watermark image
Compare the watermark Extracted and watermark generated using key.
End:
.

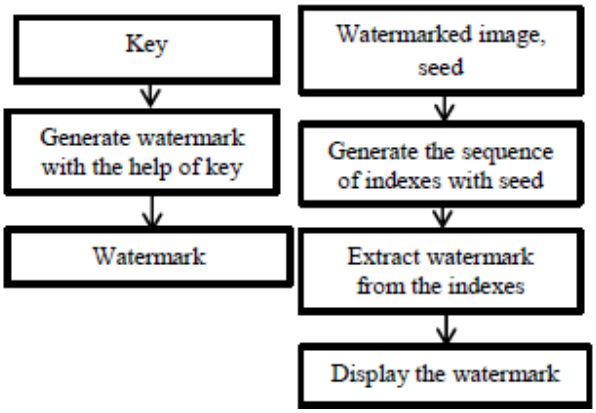

Fig.3 Recovery procedure at receiver end

III. Analysis

The algorithm is tested using PSNR (Peak Signal to Noise Ratio). PSNR is used to test the quality of the images. The higher the value of PSNR the better is the image quality.

TABLE I: COMPARISON OF PSNR VALUES OF DIFFERENT IMAGES AND DATA

S.No.	Cover Image	Embedded Data	PSNR
1	Lena	Image data 1	64.9325
		Image data 2	28.5901
		Text data	146.3432
2	Baboon	Image data 1	53.5520
		Image data 2	28.5926
		Text data	151.8969
3	Bird	Image data 1	61.7646
		Image data 2	34.9775
		Text data	168.7804

The figures represent the cover image Watermark Image or text and Watermarked image.

Fig.4Cover image

Fig.5 Watermark image

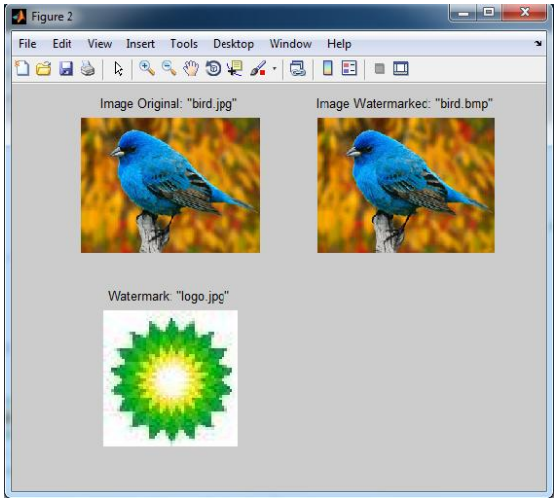

Fig.6Watermark Insertion

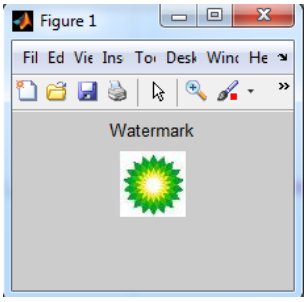

Fig.7Watermark extracted

Fig.8 Watermark as text embedded in image

IV. Conclusion

In the proposed work watermark is embedded into cover image using sequences at random indexes. The procedure will embed any type whether text or image watermark into any other suitable file such as image without actually changing the content of the carrier file. The procedure will allow to recover the data from the cover image. The procedure will be compatible with the pay load capacity of the image. The quality of the cover image is not affected by the process.

REFERENCES

[1]. Shivani Garg and Ranjit Singh " An Efficient Method for Digital Image Watermarking Based on PN Sequences" Vol. 4 No. 09 Sep 2012 International Journal on Computer Science and Engineering (IJCSE)

[2]. Ge Huayong*a,b, Huang Mingshenga, Wang Qiana "Steganography and Steganalysis Based on Digital Image2011" 4th International Congress on Image and Signal Processing

[3]. Weiqi Luo, *Member, IEEE*, Fangjun Huang, *Member, IEEE*, and Jiwu Huang, *Senior Member, IEEE*"Image watermarking based on LSB matching revisited" Ieee transactions on information forensics and security, vol. 5, no. 2,june 2010

[4]. Tsung-Yuan Liu, *Student Member, IEEE*, and Wen-Hsiang Tsai, *Senior Member, IEEE* "Generic lossless visible watermarking a new approach" IEEE transactions on image processing, vol. 19, no. 5, may 2010

[5]. Kiranmayi Penumarthi and Subhash kak " Augmented Watermarking" Cryptologia, 30:173–180, 2006 Copyright Taylor & Francis Group, LLC

[6]. Mandhani, N. and S. Kak. 2005. ''Watermarking Using Decimal Sequences,'' Cryptologia,29:50–58.