Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Embedding Data in to an Image Using Sequences

Amitoz Singh Rathore, Sur Singh Rawat
Department of CSE, JSSATE
Noida, U.P., India

Abstract:-Innovation of technology and having fast Internet makes distribution of information over the worldeasy and economical. This has made people to worry about their privacy and works. We present a techniquethat prevents unauthorized users to have access to 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 data using sequences into an Image.

Keywords: -watermark,sequence, key,secret, embedding

I. INTRODUCTION

The idea of communicating secretly is as old as communication itself. Internet communication has become an integral part of the infrastructure of today's world. The information communicated comes in numerous forms and is used in many applications. Military communication systems make increasing use of security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever security properties are provided intentionally or otherwise in the available communication 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. [2]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, it 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 [3]. In Lsb technique the data is embedded in the lower bits so that it cannot be detected by human eye at the sender end and then data is extracted at the receiver end. This method has certain drawbacks as the all the lower bits by the attacker could be changed to 1 or all the lower bits by the attacker could be changed to 0.So our data will be lost. [1]To overcome this problem we need to represent data in such a way that it appears to be random but is deterministic and there is a definite way to get it.So we can represent our data in the form of sequences. We can embed data in an image as a sequence at the sender end and extract at the receiver end.The process will comprise of 3 steps embedding procedure in which we will embed the data, the key generation process in which the key will be generated and the recovery process in which the embedded data will be recovered from the cover image.

1. *Embedding Procedure:*In order to embed the data into an image we first select the cover image then we generate the key using the data to be embedded. Next step is to convert the data that is to be embedded in the form of sequence and then we embed the data into the cover image in the form of sequence and finally we get cover image with data. The procedure is shown in figure 1 below.

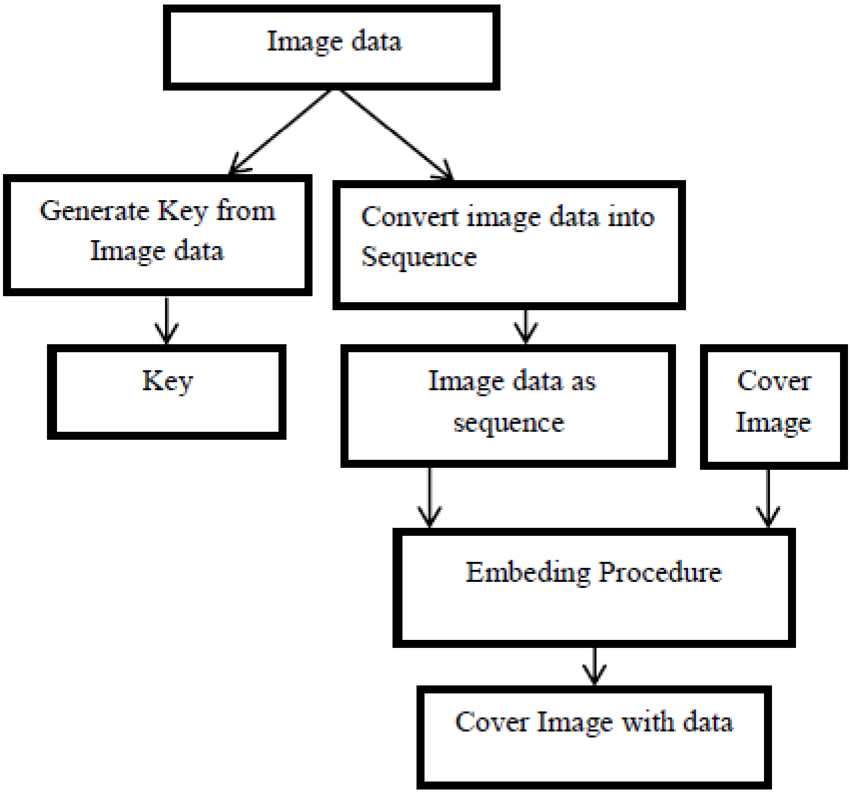


Fig. 1 Embedding Procedure at sender end

2.Key Generation: The data is embedded into the cover image using the spread spectrum technique. Let the keyto be generated by the image data be K .Consider the image data as shown in figure 2 to be an m x n image. The elements in the image are read as m × n matrix. For example, consider the following 9 × 12 image data digital sequence is shown in figure 3 to be embedded.

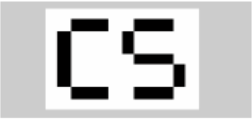
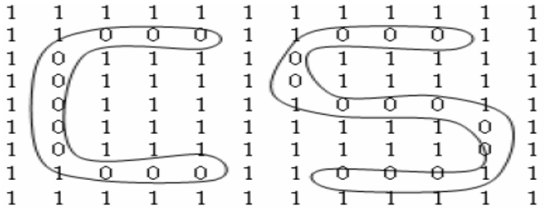


Fig. 2DataImage read in form of matrix



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

Fig. 3Digital Sequence of Data

The image data 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 1 1 0 0 0 0 0 1 1 1 0 1 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 1
1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 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 here t =5. 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 1 0 1 1 1 1 1 1

13 30 27 29 31
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
31 19 30 27 13
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
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:
K= 31 31 16 14 31 13 30 27 29 31 31 19 30 27 13 22 27 13 31 7 31 28

3.Recovery Procedure: The sender sends the key generated with the help of image data. At the receiver end the data is generated with the help of key. The image data in form of sequence is recovered. The data is converted to the image data from the sequence. The recovered data is compared with the data generated from the key. The image data is displayed. The recovery procedure is shown in figure 3 below

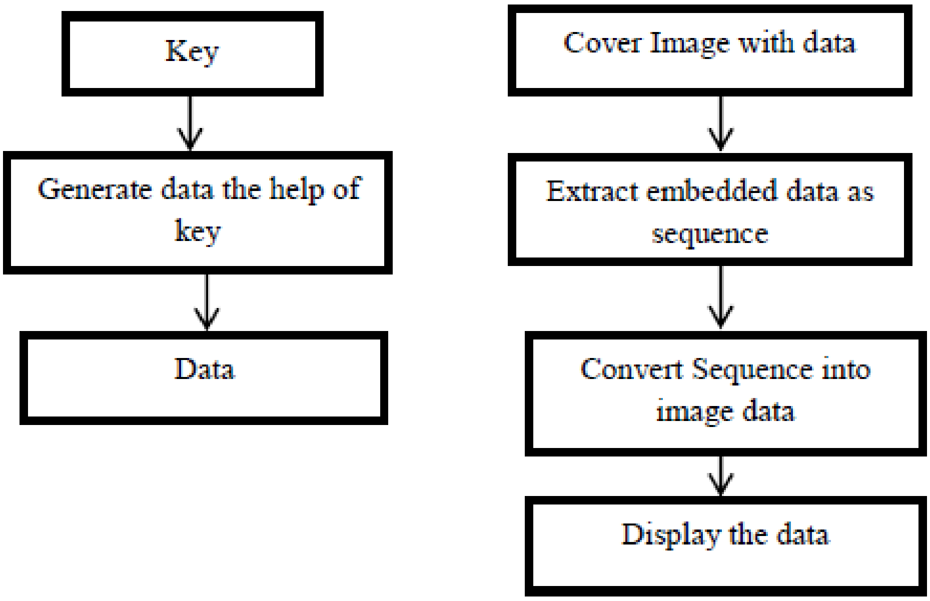

Key
Generate data the help of key
Data
Cover Image with data
Extract embedded data as sequence
Convert Sequence into image data
Display the data

Fig. 4 Recovery procedure

III. ANALYSIS

Various types of data such as image and text are embedded into the cover image and the results are analyzed as shown below. The figures represent the cover image with embedded data as Image or text.

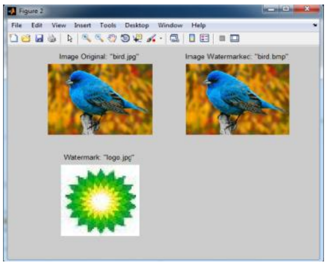
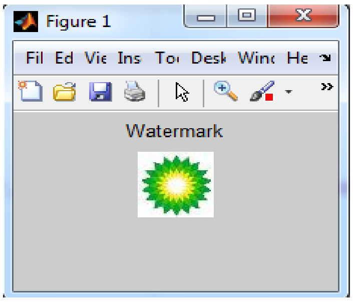


Figure 2
File Edit View Insert Tools Desktop Window Help
Image Original: "bird.jpg"
Image Watermarked: "bird.bmp"
Watermark: "logo.jpg"

Fig. 5Cover ImageFig. 6 Image DataFig. 7 Image Data Insertion



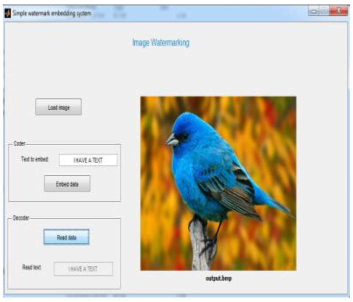


Fig.8 Image Data ExtractedFig.9 Text Data Embedded in Image

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

IV. CONCLUSION

The main objective of this work is to provide robustness and security. In the proposed work data is embedded into cover image using efficient scheme.The procedure will embed any data into any other suitable file such as image, text 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 Image will not be affected by the process.The format of the file will not be changed 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] GeHuayong*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] KiranmayiPenumarthi and Subhashkak “ 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.