Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 8; April-June, 2015 pp. 92-97

http://www.krishisanskriti.org/acsit.html

Data Encryption using Invisible Image Watermarking

Alpana Kakkar[1] and Apoorva Gupta[2]

[1,2]Amity Institute Of Information & Technology, Amity University Noida, India
E-mail: [1]akakkar@amity.edu, [2]apoorva17r@gmail.com

Abstract–*Data security is an important issue these days. From small companies to big MNCs and government organization, data security and secure data transmission is a prime requirement. There are numerous methods and algorithms for encryption but we are focusing on digital image watermarking. Watermarking is the processes of hiding data in an image in which an image is transmitted by hiding it into another image. This process is also known as image cryptography. The motive is to present this process using LSB algorithm for invisible image watermarking in which the hidden image cannot be seen by any observer or eavesdropper. The paper will initially present brief aspects of a network, network security and various attacks on network that can steal our information and after that watermarking will be introduced with the simulation performed in MATLAB.*

Key Terms*: LSB, Data encryption, Watermarking*

1. INTRODUCTION

Data needs to be encrypted to protect from various security issues and attacks to maintain integrity and and restrict access. There are various methods of data encryption or secure data encryption and one of those methods is Digital Image Watermarking. Digital Image watermarking combines the concept of Image processing with that if cryptography and it is also known as image cryptography. In Digital Image Watermarking we will hide one image (data image) into another image (cover image) and compare them on the basis of their histogram [1] [2]. We will also see that normal vision would not be able to distinguish between watermarked image and non-watermarked image. Our algorithm will include the hiding of an image into another image and retrieving the image in the form of binary image after addition of the channel noise.

Normal encryption schemes are known as Disk encryption schemes generally operating on 512 byte data sectors which can be individually encrypted or decrypted using cipher mode like CRC or cyclic redundancy check[3]. However sometimes data is needed to be accessed through the middle of the disk alone itself and its not feasible then to decrypt or encrypt depending on preveious or successive sectors[4][5].

Disk encryotion can be attacked by using watermarking attack in which an attacker can detect any encrypted. This attack make it look weaker and newer and well as older disk encryption programs, are now deprecated loop [6][7].

In an **active attack,** the attacker tries to bypass the security or break into secured system environment. This can be done through hacking, stealth, viruses, worms, or by using Trojan horses i.e. backdoor. In active attacks an attacker attempts to break or overcome protection features, to introduce or write malicious code, theft or modification of existing information [8][9].

2. LITERATURE REVIEW

2.1 Methodology

The paper is simulation based paper and simulation has been performed using MATLAB R2013b software package developed by Mathworks Inc. Matlab is an acronym for Matrix Laboratory working on interactive programming environment[10][11]. It is a very wide application tool with its domains of simulation ranging from Image Processing, signal processing to biomedical simulation. It consists of standard libraries LINPACK and EISPACK consisting of support functions files in .m format which is the file extention for matlab script files. Matlab can take anydata in form of matrix from 1 dimensional arrays to 2 dimensional matrix. It works very well with numerical data and the presence of graphical output is also available to supplement numerical results.

Our project uses Image processing applications and tools of Matlab. Matlab uses built in adaptors for accessing devices like USB cameras or Webcam for accessing realtime image captures.

Filtering is a technique for modifying, or enhancing an image. For example, you can filter an image to emphasize certain features, or remove other features. Image processing operations can be implemented with filtering, it includes smoothing, sharpening, and edge enhancement[12][13]. Filtering is a neighborhood operation, in which the value of any given pixels in a output image is determined by applying some algorithm to the expected values of the pixels in the neighborhood of the corresponding input pixels.

2.2 Background Study

Data needs to be encrypted from various security issues, and attacks to maintain the integrity, and access control. There are various methods of data encryption or secure data encryption

and one of those methods is a Digital Image Watermarking. In this paper, we are presenting the process of a Digital Image Watermarking using LSB watermarking algorithm. In this we will hide one image (data image) into the another image (cover image) and compare them on the basis of their histograms. We will also see that the normal vision would not be able to distinguish between the watermarked image and

Image processing means converting an image into its digital form by analyzing it in pixel form and perform various operations on it.Matlab takes an image as input and open it as 2D matrix and then various characteristics like its histogram and intensity can be processed.It is very rapid growing technology in present era with its applications reaching various domains from research industry to security and multimedia and communications.

2.2.1 What can be done by Image Processing ?

- Transformations in an image such as enlargement, reduction, and rotation.
- Color corrections in an image such as adjustments in brightness, conversion to different color formats like grayscale to RGB or to binary format.
- Registration or alignment of two or more than two images.
- Segmenting an image into various regions.
- Editing Images and providing Retouch and many more functions

2.2.2 Applications

The application of image processing varies within various spheres. Some of them are listed below:

- Satellite Image Processing
- Medical Imagining
- Face detection and Recognition,
- Biomedical
- Microscope image processing
- Cryptography

3. WATERMARKING

Watermarking is the process in which data in digital form is hidden in a cover image or signal. In invisible image watermarking, a message image is hidden under cover or carrier image [14][15]. The message or the data image is known as watermark as it is hidden. This particular type of digital image watermarking is also termed as invisible image watermarking. It is prominently used for tracing copyright infringements and also used for bank notes authentication. The Watermark is also applied to visible media like image or a videos, whereas the signasl or the carrier can be in any form like audio, pictures, video or text. A signal or a carrier is capable of carrying different types of watermark at the same period of time. The phenomenon of such watermarking scheme is shown in Fig. 1 and is known as visible image watermarking and its drawback is that it degrades the quality of image [16][17].

3.1 What is a watermark?

A watermark usually is a visible embedded overlay on an image in digital format which could be a form of text, a logo, or digital form of copyright notice. The main purpose of a watermark is to identify the work and prevent its unauthorized use [18][19]. However a visible watermark can't prevent unauthorized use but it do makes it difficult for those who may want to steal and claim someone else's piece of work as their own [20].

Fig. 1: Watermark Copyright

Our proposal involves invisible image watermarking. It is not the new phenomenon. Over One thousand years, the watermark on a paper has been used for a particular brand [21][22]. In a modern time, it is getting more and more important to provide authenticity as more of a worlds information is stored, as readily transferable bits. Digital watermarking is therefore, an important process, where arbitrary information, is encoded into an image in such a way that the additional payload is a imperceptible to the image observer. Hence Digital Watermarking technology is also involved with the large numbers of image processing algorithms, and also the mathematical tools [23][24]. If we use only ordinary programming tool to implement the functions of algorithm and modulation, it is very difficult. Therefore, using a high- performance science,and engineering calculation software is also very important [25] [26].

Watermarking your images and photos is an important part of protecting your online photos and images. The amount of image theft on the Internet and the growing attitude of people that everything is free for the downloading and copy paste is actually exploding the speed of the thefts. Also with the increase in technology, tools for image

repairing are available which are making it even easier to remove watermarks. This justifies the need of watermark with complex algorithms. The complex here doesn't mean to create watermark but it should be made tough for the image processing software to remove the watermarks. [27][28][29].

3.1.1 Types of Watermarking

There are several ways of classification of digital watermarking techniques:

On the basis of Robustness

- Fragile Watermarking: When a watermark fails to be detected even after the slightest modifications, the scheme of watermarking is known as fragile watermarking. These are used for tamper detection.
- Semi fragile Watermarking: When a digital watermarking resists benign transformations, but fails its detection after the transformations.
- Robust Watermarking: A digital watermarking scheme is called robust if it can resists a designated class of transformations.

On the basis of Perceptibility

- Imperceptible: When the original cover image and the marked signal are perceptually indistinguishable, the watermarking scheme is known as imperceptible watermarking
- Perceptible: When the presence of the watermark can be noticed, the watermarking scheme is known as perceptible.

On the basis of Capacity

- Zero Bit Long Watermarking: When the message os conceptually with the length of zero bit and is designed to detect whether the watermark is present or absent over the marked object, the watermarking scheme is known as zero bit long watermarking. This is also known as 1 bit scheme because the value 1 denotes the presence of the watermark and the value 0 denotes the absence of the watermark.
- Non zero bit watermarking: in this scheme unlike the above mentioned scheme, the message is n bit long strem.

On the basis of Embedding method

- Spread Spectrum: If the marked signal is obtained by an addition modification, watermarking scheme is known as Spread spectrum watermarking. They are more robust but have low information capacity.
- Quantization Type: If the digital marked signal is obtained by the process of quantization, watermarking is known quantization type. It has low robustness but high information capacity.
- AM Watermarking: When the mark signal is obtained by additive modification which is similar to the spread spectrum watermarking method but is embedded in the spatial domain.

3.2 DIGITAL WATERMARKING VS OTHER TECHNIQUES

The main basic difference between the digital watermarking and the other technologies are [30][31][32]:

i. The encryption watermarking is imperceptible, so, the image will not be detracting from the aesthetic sense.
ii. If the works are displayed, or converted into any other file formats, the watermarks will not be eliminated anymore.
iii. The watermark have exactly the same information, as information of transformation.
iv. A wide variety of techniques have been proposed, but it is very complex to measure their quality.

3.3 APPLICATIONS OF DIGITAL WATERMARKING

There are various applications of digital watermarking. Some of them are following [33][34]:

i. Protection of copyrights
ii. Source tracking
iii. Monitoring Broadcast
iv. Video authentication

I. ALGORITHM AND SIMULATION

In addition, algorithm is partitioned into couples of ways; watermark embedding algorithm, and the watermark extractions algorithm. The watermarking embedding is composed of 3 steps:

- Processing Key
- Embedded algorithm
- Watermarked pre-processing

Same way the extractions are also composed of 3 steps:

- Processing Key
- Algorithm Extraction
- Inverse watermark transformation

The above steps will be implemented in an Image Processing Tool known as MATLAB. Coding and Simulation will be done according to the MATLAB syntax. For the ease of understanding we are mentioning the step wise working of LSB Watermarking Scheme.

Step 1:- Read cover object (image) you want to use for Watermarking.
Step 2:- Read the message image (Data) you want to hide in the cover image.

Step 3:- Spread the images value on 256 gray-scale (for better efficiency).
Step 4:- Determined the size of the cover image and message object used for Watermarking.
Step 5:- Set the LSB of cover object to the value of the MSB of watermark.
Step 6:- add noise to watermarked image.
Step 7:- write to file the two images.
Step 8:- use LSB of watermarked image to recover watermark.
Step 9:- scale the recovered watermark.
Step 10:- scale and display recovered watermark.

The simulation has been performed on MATLAB. We took 2 images, one is the cover image and other one is the watermark. Our aim is to hide the watermark inside a cover image. The Fig. 2 is the cover image and Fig. 3 is showing its histogram. The Fig. 4 is our watermark image which we want to hide in cover image i.e. Fig. 4 is to be hidden in Fig. 2

Fig. 2: Cover Image

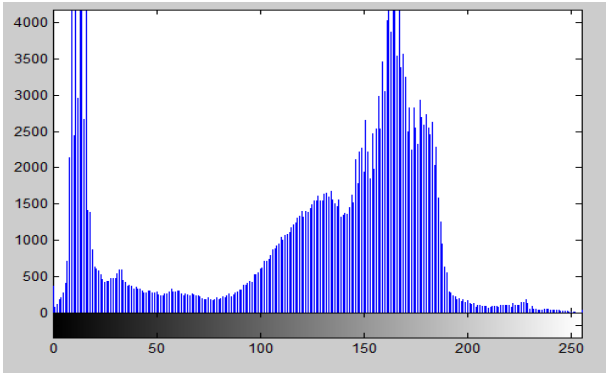

Fig. 3: Histogram of the Cover Image

We took 2 images, one is the cover image and other one is the watermark. Our aim is to hide the watermark inside a cover image. The Fig. 2 is the cover image and Fig. 3 is showing its histogram. The Fig. 4 is our watermark image which we want to hide in cover image i.e. Fig. 4 is to be hidden in Fig. 2.

Fig. 4: Watermark Image

The outcome of the LSB invisible image watermark algorithm is the Fig. 5 which is the watermarked image i.e. image in the Fig. 4 has been properly inserted in the image in Fig. 2. In the Fig. 5 i.e. the watermarked image we cannot see any watermark or the presence of watermark, this is because we are working on invisible image watermarking, however in image i.e. visible image watermarking, watermark was clearly shown in the image that also degrades the quality of the image.

On looking at Fig. 2 and Fig. 5 together, there seems no difference as such. Normal human vision may not be able to recognize that the image has been watermarked, however if we look in to the histogram of the same image which is shown in Fig. 6, we can see the differences clearly.

Fig. 5: Watermarked Image

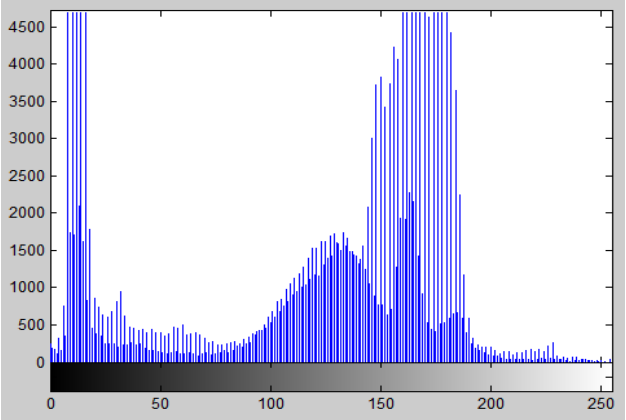

Fig. 6: Histogram of the Watermarked Image

On comparison of histogram in Fig. 2 and Fig. 6 of Fig. 2 and Fig. 5 respectively only we can show the differences between watermarked and non-watermarked images.

Fig. 7: Received watermarked Image at the destination (noisy)

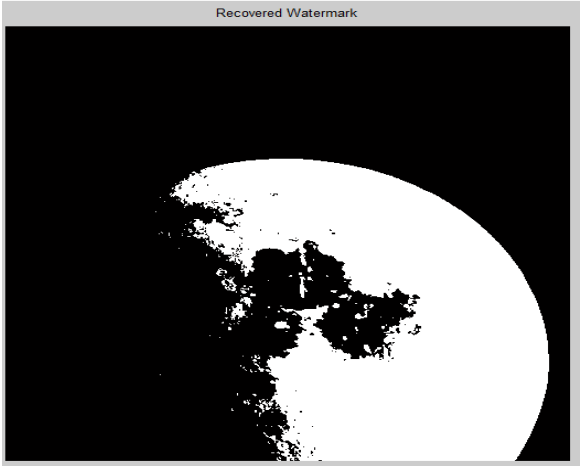

Fig. 8: Recovered Watermark in Binary Form

The above is the received image at the destination with the addition of noise as it occurs in communication channel and below is the recovered watermarked image.

4. CONCLUSION

Digital Image Watermarking is a new and merging area of research. A large variety of watermarking techniques is currently available in the literature. It mainly deals with adding hidden messages or copyright notices in digital image. These watermarks, however, are not perfect and more could be done to improve a watermark's robustness or accuracy in detection. This paper shows the stepwise process of invisible image watermarking which will be easy to understand whoever read this and will serve as a base paper for understanding the concept for the new researchers. There are lots of other technologies for Digital Image watermarking which will be discussed in future works

REFERENCES

[1] B B Zaidan, A.A Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences 10(15): 1650-1655, 2010

[2] Domenico Bloisi and Luca Iocchi, "Image Based Steganography and Cryptography", Sapienza University of Rome, Italy.

[3] Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston. London, 2000

[4] G., Derrick, (2001), Data watermarking Steganography and watermarking of digital data, Computer Law & Security Report, 17 (2), 101-104.

[5] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in Proceedings of ICIP, (Santa Barbara, CA), October 1997.

[6] P. W. Wong, "A watermark for image integrity and ownership verification," in Proceedings of Ist PIC Conference, (Portland, OR), May 1998.

[7] X. M. Niu, M. Schmucker, C. Busch. Video Watermarking Resisting to Rotation, Scaling and Translation. Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV, San Jose, CA, USA.

[8] J. Dittmann, P. Wohlmacher, K. Nahrstedt, "Approaches to Multimedia and Security: Cryptographic and watermarking algorithms", unpublished, Villacherstrasse, USA.

[9] Y. Zhang, "Digital Watermarking Technology: A Review", 2009 ETP International Conference on Future Computer and Communication, Jiangsu, China.

[10] Jeremy Kepner. Parallel MATLAB for Multicore and Multinode Computers. SIAM, 2009.

[11] James W. Demmel. Applied Numerical Linear Algebra. SIAM, 1997.

[12] Durand, F., Dorsey, J.: Fast bilateral filtering for the display of high-dynamic-range images. SIGGRAPH (2002).

[13] Itawadiya, A. K.., Mahle, R., Patel, V., Kumar D., "Design a DSP operation using Vedic Mathematics", IEEE International Conference on Communication and Signal Processing, 3-5 April, 2003.

[14] Artz, D, „Digital Steganography: Hiding data within Data", IEEE Internet Computing, May/June 2001.

[15] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag

[16] L. Reyzen And S. Russell, "More efficient provably secure Steganography" 2007.

[17] Doron Shaked, Nur Arad, Andrew Fitzhugh, Irwin Sobel, "Color Diffusion: Error Diffusion for Color Halftones", HP Laboratories Israel, May 1999.

[18] N. Provos and P. Honeyman, "Hide and Seek: An introduction to Steganography," IEEE Security & Privacy Journal 2003.

[19] Steven W. Smith, The Scientist and Engineer's Guide to Digital Signal Processing

[20] R. Gennaro, S.Jarecki, H. Krawczyk, and T. Rabin. Robust threshold dss signatures.Inf. Comput., 164(1):54{84, 2001.

[21] Zhang, X. & Wang, S. Efficient steganographic embedding by exploiting modification direction. IEEECommunications Letters, 2006, **10**(11), 781-83.

[22] Cheng, Z.; Kim, Se-Min &Yoo, Kee-Young. A new steganography scheme based on an index-colour image.*In* the 6th International Conference on Information Technology: New Generations, Las Vegas, Nevada, 2009, pp. 376-81.

[23] Younes, Mohammad Ali Bani & Jantan, A. A new steganography approach for image encryption exchange by using the least significant bit insertion. Inter. J. Comp. Sci. Network Security, 2008, **8**(6), 247-254.

[24] Anderson, Ross J. and Fabien A. P. Petitcolas. "On The Limits of Steganography." Special Issue on Copyright & Privacy Protection. IEEE Journal of Selected Areas in Communications 16.4 (1998): 474-481.

[25] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, :08, 1999

[26] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002 [8] Artz, D., "Digital Steganography: Hiding

[27] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON-2008, (2008) November, pp. 1-6.

[28] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, (2007).

[29] Darshana Mistry "Comparison of Digital Water Marking methods"(IJCSE) International Journal on Computer Science and EngineeringVol. 02, No. 09, 2010, 2905-2909.

[30] Cox, Miller and Bloom, "Digital watermarking", 1st edition 2001, San Fransisco: Morgan Kaufmann Publisher.