International Journal of Management & Information Technology
Volume 3, No 1, January, 2013

Security for Watermark Image

Prof. Dr. K. N. Barbole[1], Prof. S.D. Satav[2]
[1]Professor, Department of Electronics & Telecommunication Engineering
JSCOE, Hadapsar, Pune.
[2]Asst. Professor, Department of Computer Engineering,
JSCOE, Hadapsar, Pune.

ABSTRACT

This paper through security will improve the capacity of invisible watermarked data. The watermark image hiding secret bits of information with a digital content as a cover. Most important objectives of information hiding research are that secret information is embedding as much as possible without the perception of the carrier is affected. A hiding information algorithm of LSB bit based on high frequency domain in color image is proposed, which has high imperceptibility and high capacity of information hiding.

Keywords: Invisible Watermarking, Security, Capacity, Imperceptibility, Information hiding, LSB (Least Significant Bit)

1. INTRODUCTION

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of computer-aided information hiding in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data.

One application of digital watermarking is *source tracking*. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. With the ever-growing expansion of digital multimedia and the Internet digitizing of visual data such as images and video has become increasingly popular. However, this advancement in technology has dual impact. While, on one hand, it has enabled faster and more efficient storage, transfer and processing of digital data; on the other hand, duplication and manipulation of

digital contents has also become very easy and undetectable., which enable fast and error-free movement of any unauthorized digital data and possibly manipulated copy of such information, grow in popularity in the recent years, security concerns over copyright protection of digital multimedia data have also been increasingly emphasized. One of the most promising solutions appears to add author information (watermark) into the visual data as a secondary signal that is not perceivable and is bonded so well with the original data that it is inseparable. Digital watermarking emerged as a tool for protecting the multimedia data from copyright infringement. "Digital Watermarking can be defined as a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm." This kind of watermark contains the author and the user's information, which could be the owner" logo, serial number or control information. Digital Watermarking is very common in our everyday lives; you see watermarking in currency, government documents, stamps and many other common documents detection of the watermark or communication of the. The main use of watermarking is to provide a level of certainty about the authenticity and or ownership of a document.

2. RESEARCH PROBLEM

2.1. Problem Statement

While transferring data over the network Security is always the major issues. One of the ways to transfer data safely and authentically is watermarking. The method of invisible watermarking provides a secure data transmission over the network. Security and capacity of watermark data are very important issues to be considered. Now a day lot of research is going on to increase security and capacity of watermark data. In this paper, the security of data with the capacity increased.

2.2. Proposed System

The proposed method will increase the capacity of data that can be achieved by dividing the complete image in a series of segments. These segments are represented as the separate matrices over the image. The data will be stored in these smaller segments separately. Last 3 bits of each segment for storing the data. The storage of data depends on the high intensity pixel frequency of LSB in each area. The multiple text file added into the image and text embedding capacity depend upon image size. The security is being increased by the selection of random image segment to store the data behind the image. It means for the stegnoanalysis the intruder cannot reveal data till they do not know about the segments and the segmentation areas.

2.3. Objectives

Digital watermarking hides secret or personal information in host digital data to demonstrate and protect the copyrights of digital products, to authenticate the contents of digital data or to convey side information such as access control or annotations. To design watermarking algorithm that can embed more number of watermark bits and increase security of watermarks. Watermark is a pattern of bits inserted into a digital image that identifies the file's copyright information (author, rights, etc.). The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format.

3. METHODOLOGY OF RESEARCH

Solving the research problem through Research methodology.

3.1. Approaches for Watermarking At Frequency Domain

(1) **Resiliency against Connectivity Alterations**: Our watermarks are resilient against such common mesh-connectivity altering operations as mesh simplification and remeshing. We solved this issue by remeshing based on the connectivity of the original mesh.

(2) **Resiliency against Combined Attacks:** Our watermarks are resilient against attacks that combine cropping with geometric transformation, mesh simplification, smoothing, and other interferences. We employed the careful

alignment of possibly cropped meshes based on subsets or "patches" of the mesh

(3) **Performance Improvement**: We have improved the computational efficiency of the spectral analysis more than tenfold by adopting the Arnoldi method for Eigen value decomposition. We can now analyze and watermark meshes having tens of thousands of vertices as a single domain

There are two main approaches to research, namely quantitative approach and qualitative approach. The quantitative approach involves the collection of quantitative data, which are put to rigorous quantitative analysis in a formal and rigid manner. This approach further includes experimental, inferential, and simulation approaches to research. Meanwhile, the qualitative approach uses the method of subjective assessment of opinions, behavior and attitudes. Research in such a situation is a function of the researchers impressions and insights. The results generated by this type of research are either in non quantitative form or in the form which cannot be put to rigorous quantitative analysis. Usually, this approach uses techniques like depth interviews, focus group interviews, and projective techniques. Research approach used for this proposed work is watermarking at frequency domain. By using approach we embed invisible watermark into image called invisible watermarking. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of Steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove.

3.2. WATERMARKING EMBEDDING PROCESS

In the defined system the first work is to get the input text and the source image. Then to store data it will be converted to the raw data format i.e. represent bit system. Now the actual watermarking approach will be defined to hide data over the image. Finally the output watermarked image. Embedding process contains two modules they are data conversion and watermarking.

Data conversion: In data conversion module the given data is converted into its binary values and those binary values are changed into numeric streams because if a hacker try to get the data behind the image it cannot be understandable to him this process makes the project more secured. Data conversion is explained with the help of fig. which is given below:

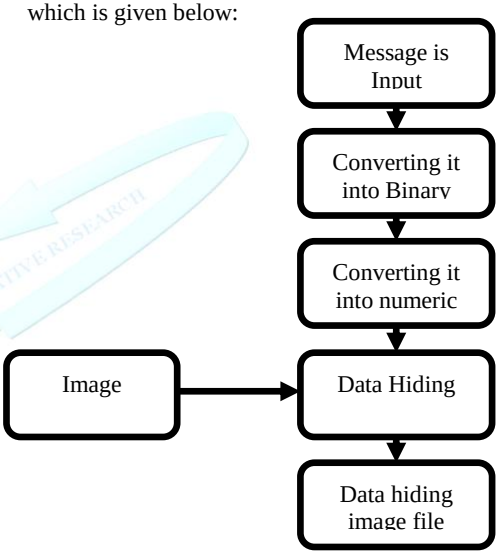


Figure 3.2 Embedding process of watermarking

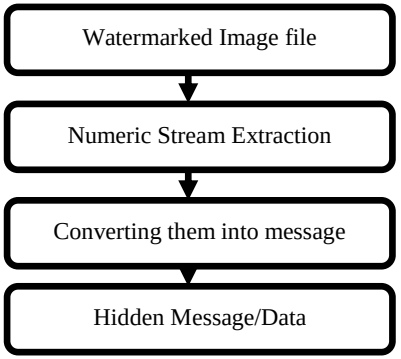


Figure 3.3 Extracting process of watermarking

Watermarking: In the module for embedding process, the word document is converted into bytes and combining the data from the above module in the word document the output is a watermarked word document.

3.3. Extraction Process

In the process the input image with data hidden inside the extracted data is in the form of numeric stream so it is converted into binary values and using that binary value the data is formed. In this extraction process the firstly the watermarked image is extracted. Now by performing the algorithm in reverse order the data is back retrieved. Once the data is retrieved in binary format the will be stored to the specified location. This extraction process is shown in above figure 3.3

4. IMPLEMENTATION

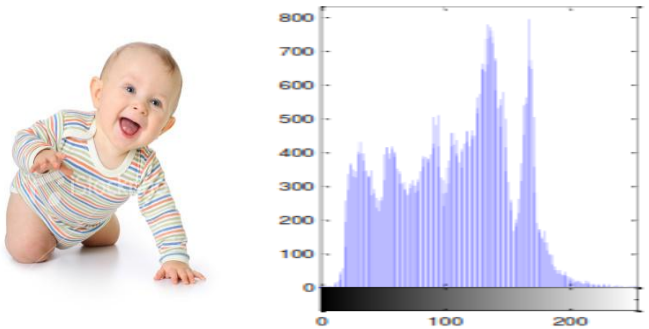
In the proposed system the technique called Matrix Encoding technique in which authentication is provided such that both objectives of efficiency and reliability are effectively controlled and achieved is used which gives the proposed system more security and efficient. The Matrix encoding method in inverse mode for the extraction process is used that extracts the data from the image without any kind of data loss.

4.1. ALGORITHM FOR EMBEDDING-EXTRACTING WATERMARK IN IMAGE

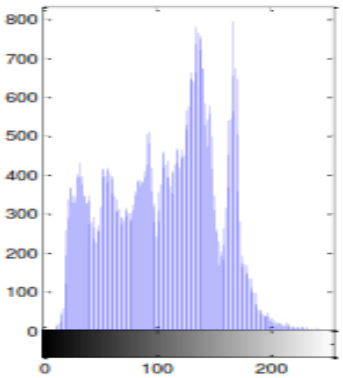
Gi (n*n): the sub image matrix. Each element of Gi will be referred to according to its row and column as P(r, c). Bi (n*n): the selected values matrix with row and column as (i, j) and embed text data, save into Bi The number (m) of bits used to hide the data could be two or three bits, so the elements of the matrix Bi will be all less than or equal to (2m-1); If a three LSBs are used to hide the data, then the elements of Bi are all less than or equal to (23 -1). The size of the matrices (n*n) is determined depending on the size of the image and the number of bits we want to hide in that image; so n could be 2, then Ki, Gi, Bi will all be of size (2*2); and we are going to embed (mbits) within (96 bit); (m could be 2 or 3 bits) If n=3 then Ki, Gi, Bi will all be of size (3*3), and we are going to embed m-bits within 216 bit; and if n=4, then we are going to embed m-bits within 384 bit; and so on. This technique similar to extracting watermark in image but these step reverse.

5. EXPERIMENTAL RESULTS

The research in the watermarked image to check image perceptual quality, histogram graph and PSNR.



Histogram Source Image



Histogram watermarked Image

In above original image and watermarked image color luminance not changes. We check that in both image histogram graphs similar. So this type of watermarking is invisible watermarking.Table1 show two images with different size and different watermark embedding capacity. In table we show that it's result of source image and watermarked image same and it's PSNR (peak signal to noise ratio) also same. According to the above result, the truly imperceptibility is satisfied fundamentally. The experiment's result also confirmed that the value of the human appreciable brightness of image not changes.

5.1. Advantage Of Invisible Watermarking System

The proposed system is secure as the data is stored in different segments of the images randomly. There is no static area to store data in image. Such as in case of LSB data is stored from the high frequency of different segment of initial of the image byte by byte. But in work the area will be selected dynamically by the proposed system itself. The proposed system is efficient. The proposed system is easy to understand with basic knowledge of the matrix system.

6. CONCLUSION

In the paper, a general coding-type framework is proposed which provides useful and constructive tools in the analysis and design of invisible watermarking system. Content management is important for protection of rights of digital multimedia creations that are distributed on the Internet. Digital watermarking is an effective technique for embedding rights information in digital multimedia data. Digital watermarking is an emerging technology which is critical for IP rights management and it is expected to have huge commercial potential when it gets widely deployed in consumer electronic devices. In particular, the effectiveness of watermarking approach in achieved with the help of design objectives such as robustness, capacity, security, and implementation efficiency. Typically proposed technique is computationally expensive, and unpredictable. This remains one of the major problems in the development of robust digital watermarking for digital images Even if the algorithm is know it is not easy to retrieve the data.

7. FUTURE SCOPE OF WORK

Watermarking is an emerging research area for copyright protection and authentication of electronic documents and media. Most of the research is going on in this field; the reason might be that there are so many images available at Internet without any cost, which needs to be protected. The watermarking technique that is proposed in the paper can be further extended by incorporating a public private key combination to store the data with authenticity. In addition the algorithm can be optimized and improved for making it faster and more intelligent. The same approach can be applied on different media like

video, audio etc. Right now the proposed approach is working only with the images.

REFERENCES

[1] Ioannis Pitas,Senior Member,IEEE"Region-based image watermarking" IEEE Transaction On Image Processing, Vol.10, No.11, November 2001

[2] Chiou-Ting Hsu and Ja-Ling Wu, Senior Member, IEEE "Hidden digital watermarks inimages" IEEE Transactions On Image Processing, Vol. 8, No. 1, January 1999.

[3] Dhruv Arya "A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques" International Journal of Scientific & Engineering Research, Volume 1, Issue 2, November-2010.

[4] Dilip Kumar Sharma, Vinay Kumar Pathak and G.P. Sahu "Digital watermarking for secure egovernment framework"

[5] FrankY. Shih, Scott Y.T. Wu "Combinational image watermarking in the spatial and frequency domains" Computer Vision Laboratory, Department of Computer Science, New Jersey Institute of Technology, Newark, NJ 07102, USA,May 2002.

[6] Hossein Rahmani, RezaMortezaei, andMohsen EbrahimiMoghaddam "A New RobustWatermarking Scheme to Increase Image Security" Electrical and Computer Engineering Department, Shahid Beheshti University, G.C., Tehran 1983963113, Iran, October 2010

[7] Hsin-Lung Wu & Jen-Chun Chang & Te-Chih Chou & Lai, Wei-Ming "A New Scheme for Data Hiding on Halftone Images" Fifth International Conference on Genetic and Evolutionary Computing, IEEE, 2011.

[8] Hsiang-Cheh Huang, Feng-Cheng Chang, Wai-Chi Fang "Reversible Data Hiding with Histogram Based Difference Expansion for QR Code Applications" IEEE 2011.

[9] J. Jeedella and H. Al-Ahmad "An Algorithm for Watermarking Mobile Phone Color Images Using BCH Code" IEEE GCC conerences & exibition, Dubainited Arab Amirates, Febuary 2011.

[10] K. Vanwasi, "Digital watermarking-steering the future of security" Edition 2001.

[11] Kalaiselvan.G, Lavanya.A, Natrajan.V "Enhancing the Performance of Watermarking Based on Cat Swarm Optimization Method" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT MIT, Anna University, Chennai. June 3-5, 2011

[12] Mansi Hasija1 ,Alka Jindal2 "Contrast of Watermarking Techniques in different domains" IJCSI International Journal of Computer Science Issues, Vol.8, Issue 3, No. 2,ISSN (Online): 16940814 ,May 2011.

[13] P.Deepika, S.Rajesh, Dr.V. Srinivasa Rao "Watermark- Based Multimedia Content Authentication" (IJAEST) International Journal of Advanced Engineering Sciences and Technologies, 2011

[14] http://www.wikipedia.org

[15] http://www.google.com