IJCSMS International Journal of Computer Science and Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231-5268
www.ijcsms.com

Digital Watermarking – A Solution for Copyright Protection of Multimedia Data

Nidhi Kandhil[1], Dr. Anil Kumar[2]

[1] Research Scholar C.M.J. University, Shillong (Meghalaya)

[2]Assistant Professor, Pt. NRS Govt. College Rohtak

Abstract

The recent progress in the digital multimedia technologies has offered any facilities in the transmission, reproduction & manipulation of data. However, this advancement has also brought the challenge such as copyright protection for content providers. Digital Watermarking is one of the proposed solutions for copyright protection of multimedia data. This technique is better than Digital Signature and other methods because it does not increase overhead. Digital Watermarking is not an older Field. There are many research are going in this field. Researchers have invented technique those increase the Security, Capacity and Imperceptibility of Watermarked Images. Here, in this Thesis our main focus is on providing robustness for web applications i.e. we provide the security to images those are stored in remote server so that unauthorized customer will not receive the image from server because the image is watermarked by using the Algorithm described in this research work and if the customer will hack the image then he / she will get the distorted image.

Keywords: *Steganography, Data hiding methods, Requirement and Feasibility Analysis.*

1. Introduction

Image watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents. The technique takes its name from watermarking of paper or money as a security measure. Digital watermarking can be a form of steganography, in which data is hidden in the message without the end user's knowledge.

A watermark can be classified into two sub-types: visible and invisible. Visible watermarks change the signal altogether such that the watermarked signal is totally different from the actual signal, e.g., adding an image as a watermark to another image.

Invisible watermarks do not change the signal to a perceptually great extent, i.e., there are only minor variations in the output signal. An example of an invisible watermark is when some bits are added to an image modifying only its least significant bits. Invisible watermarks that are unknown to the end user are steganographic.

2. Methodology

Data hashing and digital watermarking are useful for tamper detection, but at the same time these techniques have associated disadvantages. For example, a typical data hash will process an input file to produce an alphanumeric string unique to the data file. If one or more bit changes occur within this original file, thereby resulting in a modified data file, the same hash process on the modified file will produce a completely different alphanumeric. In this manner, if a trusted source calculates the hash of the original data file, subscribers can verify the integrity of the data. The subscriber simply compares a hash of the received data file with the known hash from the trusted source. If the hash results are the same, they can assign an appropriate degree of confidence to the integrity of the received data. On the other hand, if the hash results are different, they can conclude that the received data file was altered.

3. Requirement & Feasibility Analysis

Feasibility is the measure of how beneficial or practical the development of the system will be to the organization. It is a preliminary survey for the systems investigation. It aims to provide information to facilitate a later in-depth investigation.

Having gone through all measures of feasibility we report to the management to figure out if the objectives of the new system are met. If and when the objectives of the system are met and the new system is approved, then the more specific details in the proposal should be considered and approved.

4. Feasibility Considerations

There are various measures of feasibility that helps to decide whether a particular project is feasible or not. These measures include –

- Operational Feasibility
- Technical Feasibility

- Social Feasibility
- Economical and Financial Feasibility
- Legal Feasibility

5. Outline Of The Research

The central idea of the research work is to develop and implement an algorithm to produce the watermark that work on different format of images. The watermark produced by this algorithm must be fragile enough that it can be easily decoded when a proper private key or the license authentication is used. And robust enough that it can withstand different transmission parameters e.g compression filters etc. The developed algorithm tends to produce the watermark on the image which is semi transparent or semi visible which carries the properties of both the Spatial (Visible) as well as the Invisible watermark. More over the algorithm implemented using C# is very easily uploaded on web pages to secure the online images from any unauthentic attacks. The watermark developed can be applied to CD's, DVD's of images, audio, video to curb the piracy.

6. Varous Data Hiding Methods

CRYPTOGRAPHY i.e. the study of secret (*crypto*) writing (*graphy*), can be defined as the science of using mathematical algorithms to encrypt and decrypt data back. It allows two people, in a standard example known as Alice and Bob, to communicate with each other securely. This means that an eavesdropper (undesired) known as Eve will not be able to listen in on their communication. Cryptography also enables Bob to check that the message sent by Alice was not modified by Eve and that the message he receives was really sent by Alice.

A message is known as a plaintext. The method of disguising the pain-text in such a way as to hide its information is encryption and the encrypted text is also known as a cipher-text. The process of reverting cipher-text back to its original text is decryption.

This is shown in figure 2.1

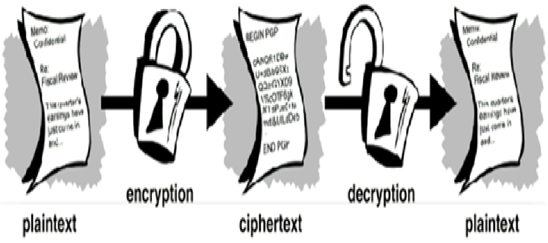

Figure 2.1: Cryptography: Conversion of Plain-Text to Cipher-Text and Reverting the Plaintext Back

While cryptography is about protecting the content of the messages, **STEGANOGRAPHY** is about concealing their very existence. Steganography comes from a Greek word that means covered writing (*stego* = covered + *graphy* = writing). Examples can be thought as messages exchanged between drug dealers via emails in encrypted forms, or messages exchanged by spies in covert communication. Steganography hides the fact that the communication ever occurred as shown in Figure 2.2.

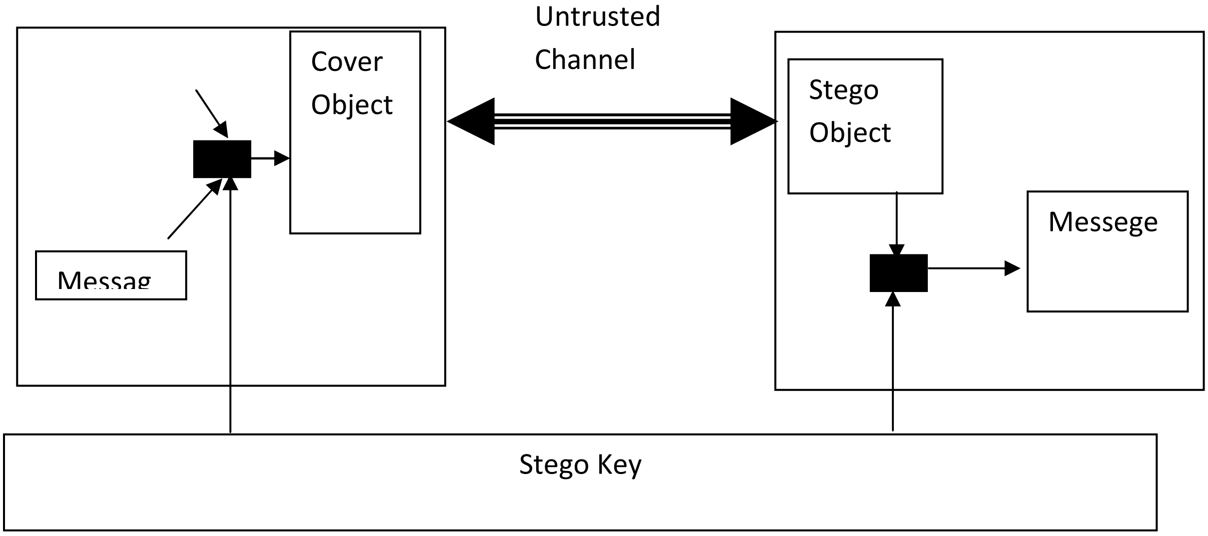

Figure 2.2: Use of Steganography for protection of text messages

Let us consider that Alice, who wants to share a secret message *m* with Bob, selects randomly a harmless message or a *cover* object *C*. The message to be shared is then embedded into *C*, by using key

K (called *stego-key*), and the cover object *C* is transformed to *stego* object *S*. This *stego* object can be transmitted to Bob without raising any suspicion. This should be done in such a way that a third party knowing only the apparently harmless message *S* cannot detect the existence of the secret. The cover object could be any data such as image files, written text or digital sound. In a perfect system, a normal cover object should not be distinguishable from the stego object, neither by a human nor by a computer looking for statistical patterns.

Alice transmits the stego object *S* to Bob over an insecure channel. Bob can reconstruct the message *m* by using the same key *K* as used by Alice during embedding the message in the cover object. The extraction process should not need any knowledge of the cover object. Any person watching the communication should not be able to decide whether the sender is sending and it covers with messages embedded into them. In other words, a person with a number of cover objects C_1, C_2 , ……, C_n should not be able to tell which cover object C_i has the message embedded in it, and the security of invisible communication lies in the inability to distinguish cover objects from the stego objects. However, not all the cover objects can be used to hide the data for covert communication, since the modifications done after the data is hidden should not be visible to anyone not involved in the communication. The cover object needs to have sufficient redundant data, which can be replaced by secret information. Although steganography and watermarking both describe techniques used for covert communication, steganography typically relates only to covert point to point communication between two parties. Steganographic methods are not robust against attacks or modification of data that might occur during transmission, storage or format conversion.

WATERMARKING, as opposed to steganography, has an additional requirement of robustness against possible attacks. An ideal steganographic system would embed a large amount of information perfectly securely, with no visible degradation to the cover object. An ideal watermarking system, however, would embed an amount of information that could not be removed or altered without making the cover object entirely unusable.

As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness.The working principle of the watermarking techniques is similar to the steganography methods. A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a key which could be either a public or a secret key. The key is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and recovery processes of watermarking are shown in Figure 2.3 and 2.4.

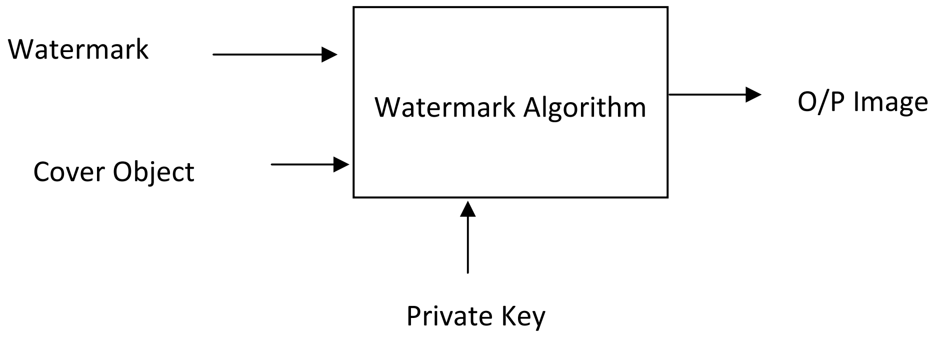

Figure 2.3: General Watermarking Block Diagram

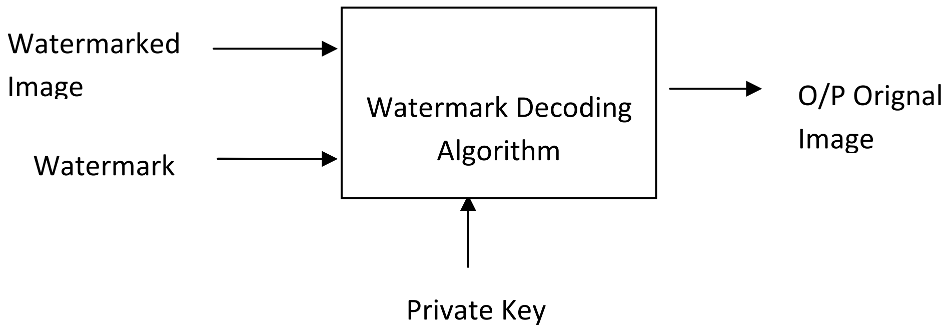

Figure: 2.4 General Watermarking Decoding to recover Original Image

For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data *W.*

The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark W.

7. Development Of Algorithm Implementation

After the deep study of various watermark technique it is emphasized that a watermark must be developed that can be directly applied to the digital image and then it can be implemented in such a way that it can be applied in connection with the modern web development techniques which can be used to curb the piracy. So learning from the various watermark techniques studied the following result has been driven.

1. The visibility of the watermark must be taken a very good care such that it must represent the copyright of the owner as well as it is invisible enough that it should not interfere with the quality of the image which has some commercial value i.e. which is for sale such as paid online images and camera digital images also.
2. It is visualized that the visibility factor **α** must be well set to satisfy our requirements of visibility of the watermark and disturbance to the image.
3. It is also learnt that in case of colored images the RGB values of image must be considered before application of the watermark on to the digital picture so that it must not produce any bad effect on the picture. That is the watermark color should be chosen such that it must not look odd when it appears over or behind the image.
4. It is also learnt that size of picture and the watermark to be applied must be matching. If the size mismatch is too large then watermark or the logo appearing on the image will look odd.
5. The position of the watermark on to the picture must be taken well care off. As Human Visibility System States that Centre of the picture is the most significant part so use of watermark on the centre should be avoided.
6. After deciding the above mentioned factors a programming language must be chosen for example if the requirement is only for the experimental purpose then use of MAT Lab is recommended as it calculates all the significant figures and the graph. However if the application demands the use of the image for commercial purposes e.g. hosting any web server or any E-Com Application then any web development language is preferred to make the program more user friendly.
7. The application of the watermark should be carefully planned and the program in chosen language should be written taking all the demanding aspects carefully.

Application: Taking all the above mentioned aspects of the watermark from the literature surveyed an application has been planned that can be implemented on E-Commerce application to curb the piracy of the digital images. The program has been written in C# using GDI classes.

8. Summary, Conclusions & Future Aspects Of The Work

The research work represents technique of watermarking making use of human visibility system at different frequencies and gazing effects on different parts of the picture. The watermark generated is semi transparent type i.e. semi visible carrying the advantages of both the visible and the invisible watermark. More over the visibility of watermark is under control of an algorithm and can be very easily changes as per changing requirements. It carries the advantage of the visible watermark i.e. it is robust and easily visible hence easy to detect the copyright on to the picture. It carries the advantages of non visible watermark also i.e. it does not interfere with the picture elements. It is manually designed by taking care of the picture statistic i.e. value of RGB and W components and more over it is placed on part of the picture which is not so significant portion. The RGB components of part of the picture have been first calculated by deciding the region where it is to be placed than by differentiating that region in pixels. The size of the watermark is always cropped to fit to that region. Unlike other watermarking algorithm visible or not visible which fixes a method of the application the proposed method is very flexible and under our control so can be very easily match the application requirements. The robust results from the methods are expected as the watermark is normally is to be applied on the periphery region of the image to be watermarked. The proposed technique is compatible and can be programmed with latest user friendly languages which are in connection with the latest online, E-Commerce and shopping applications as given in the example. More over the proposed method can be applied to all types of image formats e.g. jpeg, bmp etc.

While testing the algorithms, the computational complexity of the algorithms is not taken into account, since the main application is assumed as the copyright protection. As noted, the computational cost and memory requirements are not a priority in copyright protection. The owner of the content may want to prove his/her ownership, whether it takes days to complete the watermark detection process. In contrast to the case, if the same idea is used in a broadcast monitoring application, the algorithm should surely take those requirements into account. Although formal tests are not performed, the complexity of algorithms is not demanding.

References:

[1] Anand Deepthi, Niranjan, “Watermarking Medical Images with Patient Information”, proceedings of 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vol. 20, No 2.pp. 703-706,1998.

[2] Berghel Hal, O’Gorman Lawrence, “Digital Watermarking“, 1997, IEEE, Computer, 29:7, pp. 101-103.

[3] Gersho A. and Gray R. M, ”Vector Quantization and Signal Compression”, Kluwer Academic Publisher, London England, 1992.

[4] Hartung Frank, Kutter Martin, “Multimedia Watermarking Techniques”, Proceedings of The IEEE, Vol. 87, No. 7, July1999, pp. 1085 – 1103.

[5] Koz Alper, “Digital Watermarking Based on Human Visual System”, The Graduate School Of Natural and Applied Sciences, The Middle East technical University, pp 2-8,Sep2002.

[6] Kutter Martin and Jordan Fredric, “Digital Watermarking Technology”, In Alp Vision, Switzerland, pp 1-4, July 1999.

[7] Lu Ze-Ming, Xu Dian-Guo, Sun Sheng-He, “Multipurpose Image Watermarking Algorithm Based on Multistage Vector Quantization”, proceedings of IEEE Transactions on Image Processing, vol. 14, no. 6, pp. 822 – 830, June 2005.

[8] Nikolaidis.A, Tsekeridou. S, Solachidis .V, “A Survey on Watermarking Application Scenarios and related attacks”, proceedings of IEEE International Conference on Image Processing, Vol. 3, pp. 991-993, Oct 2001.

[9] Er-Hsien Fu, "Literature Survey on Digital Image Watermarking". EE381K Multidimensional Signal Processing.

[10] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques",Proc. IEEE, Vol.87, no.7, pp 1079-1107, 1999

[11] Wai Chu, "DCT-Based Image Watermarking Using Sub sampling." IEEE Transactions on Multimedia, Mar. 2003. pp. 34-38.

[12] Min-Jen Tsai, Hsiao-Ying Hung, "DCT and DWT-Based Image Watermarking by Using Sub sampling" Proceedings of the 24thInternational Conference on Distributed Computing Systems Workshops, MNSA (ICDCSW'04), March 23 - 24, 2004, Hachioji, Tokyo, Japan, pp. 184-189.

[13] Xiangui Kang, Jiwu Huang, Yun. Q.Shi, and Yan Lin, "A DWT-DFTComposite Watermarking Scheme Robust to both affine Transformation and JPEG Compression", IEEE transactions on Circuits and Sysytemsfor Video Technology, Vol.13, no.8, August 2003

[14] Meerwald, P., and A.Uhl, " A survey of Wavelet-Domain Watermarking Algorithms,"

in P.W. Wong and E.J. Delp, (eds.), Proceedings ofelectronic Imaging 2001, Security and Watermarking of MultimediaContents III, San Jose, CA, January 2001, pp. 505-516.

[15] Inoue, H., et al. " A Digital Watermark Technique Based on the Wavelet Transform and its Robustness on Image Compression and Transformation, "Proceedings of the 1998 IEEE International Conference on Image Processing(ICIP-98), Vol.2, Chicago, October 1998,pp. 391-395.

[16] Wang, H.-J.M., P.-C.Su, and C.-C. J.Kuo, "Wavelet Based Digital Image Watermarking," Optics Express 491, Vol.3, No.12, December1998.