High Capacitive & Confidentiality Based Image Steganography & Watermarking Using Private "Stego Key"

Abhilasha Malviya[1], Asst. Prof. Nitin Lonbale[2]
[1]*M-Tech Research Scholar,* [2]*Research Guide, Department of Electronics & Communication*
Shri Balaji Institute of Technology & Management, Bhopal

Abstract - One of the most important properties of (digital) information is that it is in principle very easy to produce and distribute unlimited number of its copies. This might undermine the music, film, book and software industries and therefore it brings a variety of important problems concerning the protection of the intellectual and production rights that badly need to be solved. The fact that an unlimited number of perfect copies of text, audio and video data can be illegally produced and distributed requires studying ways of embedding copyright information and serial numbers in audio and video data. Watermarking is one of the main methods of the fast developing area of information hiding. The main goal of watermarking is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot remove or replace mind. The goal of watermarking is to hide message in one-to-many communications. Data hiding embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions, e.g., lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party. We explore both traditional and novel techniques for addressing the data-hiding process and evaluate these techniques in light of three applications: copyright protection, tamper proofing, and augmentation data embedding.

Keywords:-Digital Image Watermarking & Image Steganography.

I. INTRODUCTION

The information hidden by a watermarking system is always associated to the digital object to be protected or to its owner while steganographic systems just hide any information "Robustness" criteria are also different, since steganography is mainly concerned with detection of the hidden message while watermarking concerns potential removal by a pirate Steganographic communications are usually point-to- point (between sender and receiver) while watermarking techniques are usually one-to-many.

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 hiding digital information 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 robustness 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.

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

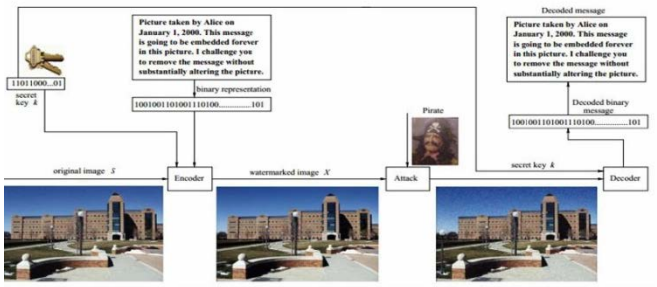

Fig. 1: Hiding Data in Images

II. FEATURES AND APPLICATIONS

Data-hiding techniques should be capable of embedding data in a host signal with the following restrictions and features. The host signal should be non-objectionably degraded and the embedded data should be minimally perceptible. (The goal is for the data to remain hidden. As any magician will tell you, it is possible for something to be hidden while it remains in plain sight; you merely keep the person from looking at it. We will use the words hidden, inaudible, imperceivable, and invisible to mean that an observer does not notice the data even if they are perceptible.

The embedded data should be directly encoded into the media, rather than into a header or wrapper, so that the data remain intact across varying data file formats.The embedded data should be immune to modifications ranging from intentional and intelligent attempts at removal to anticipated manipulations, e.g., channel noise, filtering, re-sampling, cropping, encoding, lossy compressing, printing and scanning, digital-to-analog (D/A) conversion, and analog- to-digital (A/D) conversion etc.

Asymmetrical coding of the embedded data is desirable, since the purpose of data hiding is to keep the data in the host signal, but not necessarily to make the data difficult to access. Error correction coding1 should be used to ensure data integrity. It is inevitable that there is degradation to the embedded data.

The embedded data should be self-clocking or arbitrarily re-entrant. This ensures that the embedded data can be recovered when only fragments of the host signal are available, e.g., if a sound bite is extracted from an interview, data embedded in the audio segment can be recovered. This feature also facilitates automatic decoding of the hidden data, since there is no need to refer to the original host signal.

III. SYSTEM MODEL

Different approaches may be employed to use the watershed principle for image segmentation. Local minima of the gradient of the image may be chosen as markers, in this case an over-segmentation is produced and a second step involves region merging. Marker based watershed transformation make use of specific marker positions which have been either explicitly defined by the user or determined automatically with morphological operators or other ways.

Meyers Flooding Algorithm

One of the most common watershed algorithms was introduced by F. Meyer in the early 90's. The algorithm works on a gray scale image. During the successive flooding of the grey value relief, watersheds with adjacent catchment basins are constructed. This flooding process is performed on the gradient image, i.e. the basins should emerge along the edges. Normally this will lead to an over-segmentation of the image, especially for noisy image material, e.g. medical CT data. Either the image must be pre-processed or the regions must be merged on the basis of a similarity criterion afterwards. A set of markers, pixels where the flooding shall start, are chosen. Each is given a different label. The neighboring pixels of each marked area are inserted into a priority queue with a priority level corresponding to the gray

level of the pixel. The pixel with the highest priority level is extracted from the priority queue. If the neighbors of the extracted pixel that have already been labeled all have the same label, then the pixel is labeled with their label. All non-marked neighbors that are not yet in the priority queue are put into the priority queue.

Redo step 3 until the priority queue is empty. The non-labeled pixels are the watershed lines.

Watersheds as optimal spanning forest have been introduced by Jean Cousty et al.They establish the consistency of these watersheds: they can be equivalently defined by their "catchment basins" (through a steepest descent property) or by the "dividing lines" separating these catchment basins (through the drop of water principle). Then they prove, through an equivalence theorem, their optimality in terms of minimum spanning forests. Afterward, they introduce a linear-time algorithm to compute them. It is worthwhile to note that similar properties are not verified in other frameworks and the proposed algorithm is the most efficient existing algorithm, both in theory and practice.

Overview of GUI

A graphical user interface (GUI) is a graphical display in one or more windows containing controls, called components that enable a user to perform interactive tasks. The user of the GUI does not have to create a script or type commands at the command line to accomplish the tasks. Unlike coding programs to accomplish tasks, the user of a GUI need not understand the details of how the tasks are performed. GUI components can include menus, toolbars, push buttons, radio buttons, list boxes, and sliders—just to name. GUIs created using MATLAB® tools can also perform any type of computation, read and write data files, communicate with other GUIs, and display data as tables or as plots.

The GUI contains-

An Axes Component

A pop-up menu listing three data sets that correspond to MATLAB functions: peaks, membrane, and since a static text component to label the pop-up menu three buttons that provide different kinds of plots: surface, mesh, and contour

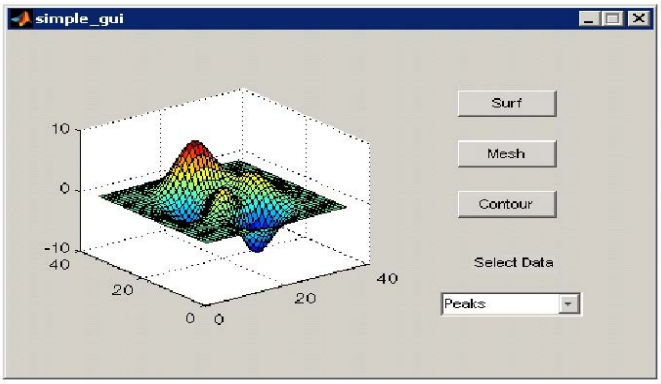

Fig. 2: Simple GUI

When you click a push button, the axes component displays the selected data set using the specified type of 3-D plot

IV. RESULTS AND DISCUSSION

This chapter presents brief overview of the tool used, design specification, simulation methodology and simulation results of the project. This chapter concludes with the comparison of all the simulated results and further provides the applications in which our project can be used.

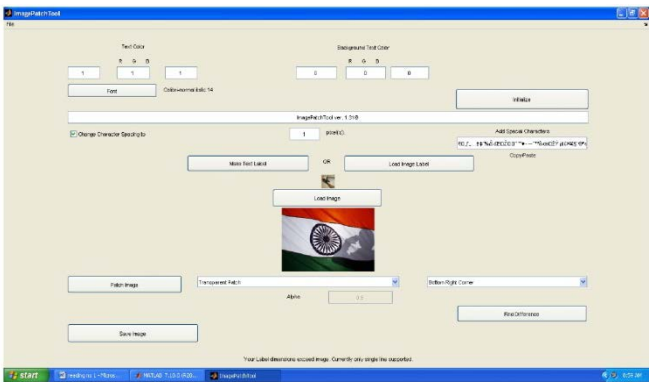

Fig.3: Overview of final GUI

V. PROPOSED METHODOLOGY

The following are the steps that are used for this project work

- *Making of GUI.*
- *Program coding.*
- *Initializing characters.*
- *Load image1/text1.*
- *Load image2/text2.*
- *Patching of image.*

Use alpha bending to vary the value of alpha and acquire different results of the watermarked output.

Text on Image

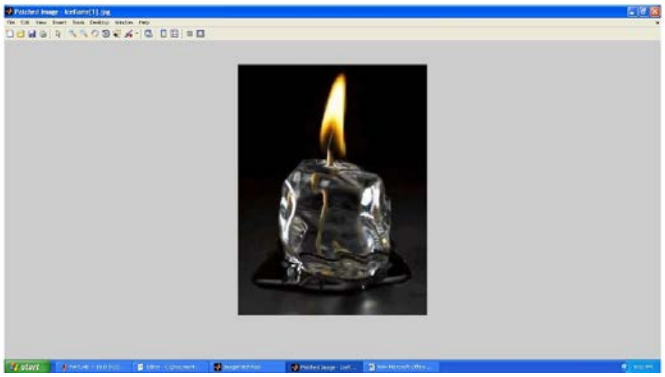

Fig. 4: Patching results for alpha =0.0

As shown in figure for the value of alpha=0 the text on the image is completely hidden

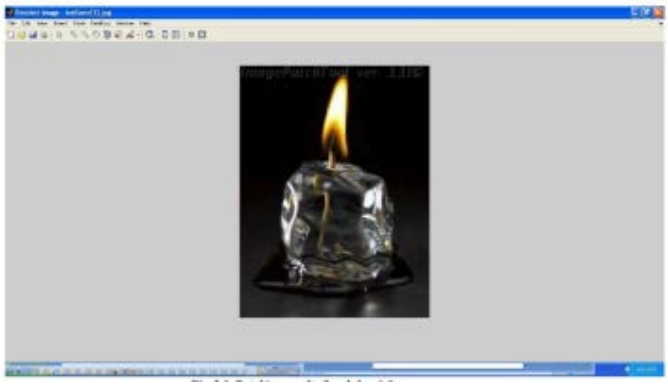

Fig.5: Patching results for alpha=0.2

As shown in figure for the value of alpha=0.2 the text on the image is not completely hidden. The text is seen blurred on the image.

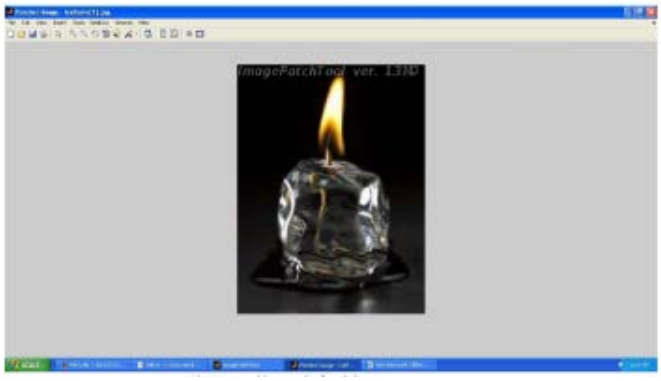

Fig.6 :Patching results for alpha=0.4

As shown in figure for the value of alpha =0.4 the text is not completely hidden though it is more vivid clear than for the value of alpha=0.2

Fig.7: Patching results for alpha=0.6

As shown in figure for the value of alpha=0.6 the text is not completely hidden though the text is more vivid clear than for the value of alpha=0.4

Fig.8: Patching results for alpha =0.8

As shown in figure for the value of alpha=0.8 the text is not completely hidden though the text is more vivid clear than for the vale of alpha=0.6

Fig.9: Patching results for alpha=1

As shown in figure for the value of alpha=1 the text is

completely visible on the screen than any other values of alpha.

Image With Image

Fig.10: Patching results for alpha=0.0

As shown in figure for the value of alpha=0.0 the desired image is completely hidden on the second image

Fig.11: Patching results for alpha=0.2

As shown in figure for the values of alpha=0.2 the desired image is not completely hidden. The desired image is slightly visible. Hence this is not complete watermark.

Fig.12: Patching results for alpha=0.4

As shown in figure for the values of alpha=0.4 again the desired image is not Completely hidden, in fact it is more vivid clear than for the value of alpha=0.2

Fig.13 :Patching results for alpha=0.6

As shown in figure for the value of alpha=0.6 the desired image is not completely hidden, infact the desired image is more vivid clear than for the value of alpha=0.4.

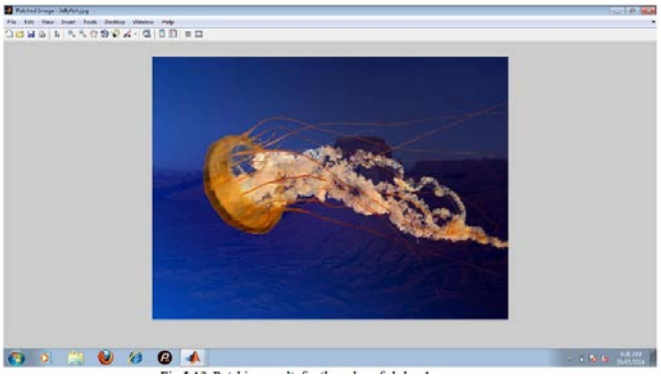

Fig.14: Patching results for the value of alpha=1

VI. CONCLUSION

This research work presents multiple aspects of data hiding with both analytic study and experimental Results. We have shown that multimedia data hiding can be used for various Applications, including ownership protection, alteration detection, and access/copy control, annotation, and conveying other side information. In addition to the design issues, we discussed attacks on watermarking algorithms with a goal of identifying weaknesses and limitations of existing design/framework as well as proposing improvements. This study would lead to a basis for designing practical media security systems, and to solutions of the Digital Rights Management (DRM) for digital multimedia data. In addition, regarding the gap between the highly simplified channel models and the real-world

scenarios in today's data hiding research, a rigorous analysis of the capacity versus robustness of data hiding in a realistic setting and incorporating perceptual Models is worthwhile to pursue. Besides the classic use in ownership protection and copy/access control, we have demonstrated that data hiding can be a useful tool to send side information in video communication.

VII. FUTURE SCOPE

Watermarking can be further spread over a vast stretch that includes the following streams The protection of intellectual property through technical means was presumably one of the primary motivations for applying well-known steganographic techniques. Protective measures can be grouped into two broad categories. The first category encompasses the protection against misappropriation of creations by other content providers without the permission of or compensation of the rights owner, while the second category includes protection mechanisms against illicit use by end users.

Misappropriation by other content providers can, in turn, occur in several forms. In the simplest case, a creation is duplicated, redistributed, or resold in its entirety and in its original form. Here, the legal framework provides, in its current form, protection even without the creation being marked with a copyright notice, though certain national jurisdictions may provide elevated protection status for creations affixed with a formal copyright notice. All three encoding and decoding schemes require that the modified output signal be compared to the original signal to attempt to recover the encoded message. Obtaining the original signal can be cumbersome in practice and may present logistical problems. Fortunately, this requirement can be lifted with a slight design change. Our algorithms could survive cropping if we set up a matched filter in the decoder. First we would determine where the marked signal is located in the original signal using cross-correlation. Then we could crop the original signal in order to compare it to the marked signal and recreate the message (without, of course, the bits lost in the crop). This project could also be furthered by creating a decoding process which takes in a signal and a message and attempts to discover whether the signal has been marked with that message

REFERENCES

[1] F. Mintzer, et al., "Effective and ineffective digital watermarks", *Proc. IEEE Int. Conf. Image Processing*, vol. 3, pp.9 -13 1999

[2] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen", *IEEE Computer*, vol. 31, pp.26 -34 2004

[3] R. A. Ulichney, *Digital Halftoning*, 2004 :MIT Press

[4] Z. Baharav and D. Shaked, "Watermarking of dither halftoned images", *Proc. SPIE*, pp.307 -313 2006

[5] K. T. Knox, *Digital watermarking using stochastic screen patterns*,

[6] S. G. Wang, *Digital watermarking using conjugate halftone screens*,

[7] R. T. Tow, *Methods and means for embedding machine readable digital data in halftone mages*,

[8] B. E. Bayers, "An optimum method for two level rendition of continuous tone pictures", *Proc. IEEE Int. Communication Conf.*, pp.2611 -2615 2007

[9] R. W. Floyd and L. Steinberg, "An adaptive algorithm for spatial grayscale", *Proc. SID*, pp.75 - 77 2007

[10] L. M. Chen and H. M. Hang, "An adaptive inverse halftoning algorithm", *IEEE Trans. Image Processing*, vol. 6, pp.1202 - 1209 2008

[11] Z. Fan and R. Eschbach, "Limit cycle behavior of error diffusion", *Proc. IEEE Int. Conf. Image Processing*, vol. 2, pp.1041 -1045 2008

[12] Z. Xiong, et al., "Inverse halftoning using wavelets", *Proc. IEEE Int. Conf. Image Processing*, vol. 1, pp.569 -572 2008

[13] Dr.V.Khanaa, IJECS Volume 2 Issue 3 March 2013 Page No. 558- 568

[14] Digital watermarking device,Leung hon yin, Dr.L.M.Cheng

[15] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992-3006, Oct. 2009

[16] D. Kundur and K. Karthik, "Video finger printing and encryption principles for digital rights management," *Proceedings IEEE*, vol. 92, no. 6, pp. 918-932, Jun. 2010