ENCODING AND DECODING TO TRACING THE SEQUENTIAL MULTIPLE WATERMARKING

Ms.B.Vinitha[1], Mr.M.Sanjheeviraaman[2], Ms.A.Tamilselvi[3]
[1]Student, MCA, [2,3]Assistant Professor
[1,2]Department of Computer Applications, Shanmuga Industries Arts and Science College, Tiruvannamalai, TamilNadu, India
[3]Department of Computer Science, Aruna Vidhya Arts and Science College, Kannakurukkai, Tiruvannamalai, TamilNadu, India

Abstract: The possibility of adding several watermarks to the same image would enable many interesting applications such as multimedia document tracking, data usage monitoring, and multiple property management. In this paper, we present a novel water marking scheme, which allows inserting and reliably detecting multiple watermarks sequentially embedded into a digital image. Also, the text can be hidden in the image, which can be read only by the user having the valid key, thus enhancing security. The proposed method, based on elementary linear algebra, is asymmetric, secure under projection attack and robust against distortion due to basic operations such as storage, transmission, and format conversion. Digital watermarking is a process for modifying physical or electronic media to embed a machine-readable code into the media. The media may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. Most commonly, digital watermarking is applied to media signals such as images, audio signals, and video signals. However, it may also be applied to other types of objects, including documents, software, multi-dimensional graphics models, and surface textures of objects. Digital watermarking systems typically have two primary components: an encoder that embeds the watermark in a host media signal, and a decoder that detects and reads the embedded watermark from a signal suspected of containing a watermark. The encoder embeds a watermark by altering the host media signal. The reading component analyzes a suspect signal to detect whether a watermark is present. In applications, where the watermark encodes information, the reader extracts this information from the detected watermark.

Keywords: watermarking, encoder, decoder

I. INTRODUCTION

Digital watermarking is a process for modifying physical or electronic media to embed machine-readable code into the media. The media may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. Most commonly, digital watermarking is applied to media signals such as images, audio signals, and video signals. However, it may also be applied to other types of media objects, including documents (e.g., through line, word or character shifting), software, multidimensional graphics models, and surface textures of objects. Digital watermarking systems typically have two primary components: an encoder that embeds the watermark in a host media signal, and a decoder that detects and reads the embedded watermark from a signal suspected of containing a watermark (a suspect signal). The encoder embeds a watermark by altering the host media signal. The reading component analyzes a suspect signal to detect whether a watermark is present. In applications where the watermark encodes information, the reader extracts this information from the detected watermark. The large use of networked multimedia system has created the need of "Copyright Protection" for different digital medium as images, audio clips, videos etc. The term "Copyright Protection" involves the authentication of ownership and identification of illegal copies of digital media. Though digital media provides various efficient facilities like distribution, reproduction and manipulation of images, audio clips and videos, they increase illegal copying of digital media. The method operates on a sample image, which is blurred and having less resolution by applying preprocessing filters to the image on which watermark has to be applied after preprocessing an enhanced version of image will be populated in the main file dialogue of the Image Processing library. Now on this image a text watermark is applied to add company name or website url again an image watermark is applied to this changed document for watermarking or embedding an image like logo of the company. After this post processing is done to give the final enhanced output with both text and image watermarks.

Digital watermarking technique is already in use by individuals and firms, but the problem here is single watermarking technique which provides low security. This has been overcome by using the multiple watermarking technique and c# languages by using this we can provide security when compared to the single watermarking.

II. LITERATURE SURVEY

More recently, different watermarking techniques and strategies have been proposed in order to solve a number of problems, ranging from the detection of content manipulations, to information hiding (steganography), to document usage tracing. In particular, the insertion of multiple watermarks to trace a document during its lifecycle is a very interesting and challenging application. The main objective is to grant the possibility of directly detecting from the document who was the creator, who had access to the data after its creation, how the propertyof the document is shared among different users, allowing not only the document tracing (crucial for example in the management of images connected to a legal prosecution), but also data usage monitoring (useful in newspaper documents processing).There are various spatial and frequency domain techniques used for adding watermarks to and removing them from signals. Purely spatial techniques are not robust to some attacks to the signal like cropping and zooming, whereas most frequency domain techniques and mixed-domain techniques are quite robust to such attacks. Securing Images with Digital Watermark. The proliferation of digitized media (audio, image, and video) is creating a pressing need for copyright enforcement schemes that protect copyright ownership. Conventional cryptographic systems permit only valid key holders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. Therefore, conventional cryptography provides little protection against data piracy, in which a publisher is confronted with unauthorized reproduction of information. A digital watermark is intended to complement cryptographic processes. It is a visible, or preferably invisible, identification code that is permanently embedded in the data and remains present within the data after any decryption process. The secret key is used to generate the random sequence. In order to be effective, a watermark should have the characteristics outlined below. The watermark should be perceptually invisible, or its presence should not interfere with the work being protected. Robustness: The watermark must be difficult (hopefully impossible) to remove. In particular, the watermark should be robust in the following areas: - Common signal processing: The watermark should still be retrievable even if common signal processing operations are applied to the data.

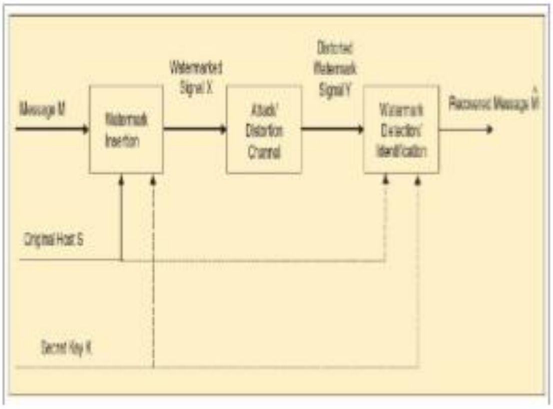

Message M
Watermark Insertion
Watermarked Signal X
Attack/ Distortion Channel
Distorted Watermark Signal Y
Watermark Detection/ Identification
Recovered Message $\hat{M}$
Original Host S
Secret Key K

Fig : Communication of a Digital Watermark

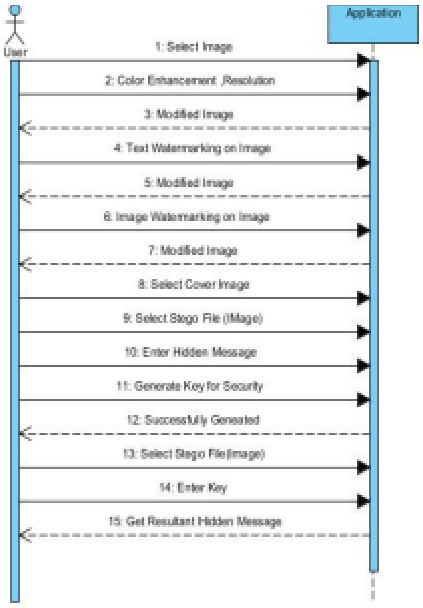
The communication of a digital watermark may be viewed as an exercise in digital communication. The message bits are encoded and embedded in a suitable carrier. The properties that are desired of the watermark, such as imperceptibility, robustness to noise and to image editing such as cropping and rotation are the factors that drive the choice of carrier. In robust watermarks, it is the combination of low signal amplitude (because the watermark is invisible) and large bandwidth (because images are typically quite large), as well as the relatively short length of the message, that dictates the use of spread spectrum for encoding the message bits. Spread spectrum is a robust and secure form of communication. In image watermarking, the spread spectrum signal is typically placed in the frequency domain to produce a watermark that is immune to image processing.

Image compression techniques, such as JPEG, inspired the use of the frequency domain for embedding imperceptible watermarks in images. The first frequency domain technique was devised by Scott Burgett, Eckhard Koch, and Jian Zhao, who utilized the Discrete Cosine Transform. This and other transforms, such as the Wavelet transform, were used by Joseph O Ruanaidh, who later developed rotation and translation invariant watermarks based on the Fourier transform. Ingemar Cox popularized the use of Spread spectrum techniques for robust watermarking. Geoff Rhoads, Chief Technical Officer and founder of Digimarc Corporation, developed the PictureMarc technology.

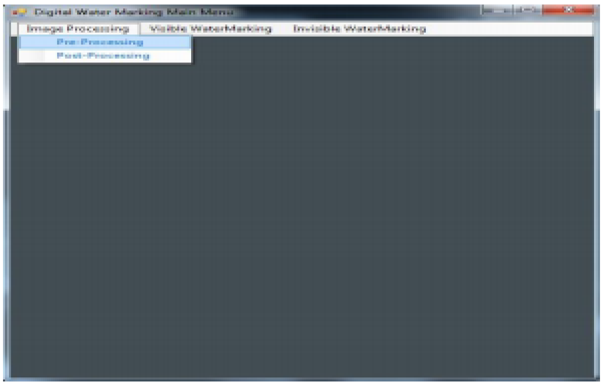
The proposed method, based on elementary linear algebra, is asymmetric, involving a private key for embedding and a public key for detection. Its robustness against standard image degradation operations has been extensively tested and its security under projection attack has also been proven even though the envisaged application refers to a collaborative environment, in which malicious attacks are not a critical aspect. Here we are providing multiple watermarking concepts, such as the sample image overwrite more than one time on the original image.

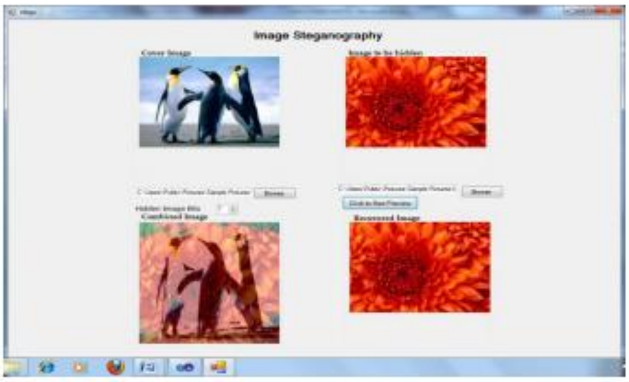
The implementation part is the most important phase of the project. In this phase we code the entire project in the chosen software according to the design laid during the previous phase. The code has to be in such a way that the user requirements are satisfied and also not complicated for the user i.e., the user interface or GUI has to be easy to navigate. The code should be efficient in all terms like space, easy to update, etc. In this manner, we can complete the coding part of the project and later it can be sent for testing before being delivered to the customer.

DESIGN


User
Application
1: Select Image
2: Color Enhancement ,Resolution
3: Modified Image
4: Text Watermarking on Image
5: Modified Image
6: Image Watermarking on Image
7: Modified Image
8: Select Cover Image
9: Select Stego File (IMage)
10: Enter Hidden Message
11: Generate Key for Security
12: Successfully Genrated
13: Select Stego File(Image)
14: Enter Key
15: Get Resultant Hidden Message

RESULTS





III. CONCLUSION

Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms. To provide a comprehensive disclosure without unduly lengthening the specification, applicants incorporate by reference the patents and patent applications referenced above. The methods, processes, and systems described above may be implemented in hardware, software or a combination of hardware and software. For example, the auxiliary data encoding processes may be implemented in a programmable computer or a special purpose digital circuit. Similarly, auxiliary data decoding may be implemented in software, firmware, hardware, or combinations of software, firmware and hardware. The methods and processes described above may be implemented in programs executed from a system's memory (a computer readable medium, such as an electronic, optical or magnetic storage device). The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

REFERENCES

[1] RafealsC.Gonzalez,RichardE.Woods, Digial Image Processing, Second Edition, Pearson Education/PHI.

[2] Fabien A.P.,andPetitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”,2000.

[3] F.Hartung, M.Kutter, “Multimedia Watermarking Techniques”, 4 Proceeding of the IEEE,Vol.87 No 7,1999,pp.1079-1107.

[4] B. Chanda, D.DattaMajumder, Digital Image Proceeing and Analysis, Prentice Hall India, 2003.

[5] Grady Booch, James Rumbaugh, Ivar Jacobson, “The Unified Modelling Language User Guide”, Pearson Education.

Authors:

Ms.B.Vinitha, student, studying in MCA, Department of Computer Applications, Shanmuga Industries Arts and Science College, Tiruvannamalai, TamilNadu , India. My research are involves Network, Cloud Computing and Network Security. I did this Journal Paper under the guidance of my project guide Mr.M.Sanjheeviraaman, his motivation is to be too good and i proud to do this paper under his excellence.

Mr.M.Sanjheeviraaman, M.Sc., M.C.A., .M.Tech., M.phil., I completed his Bachelor degree(Mathematics) in Arignar Anna Govt. Arts College from University of Madras, M.Sc Mathematics in Distance Education from University of Madras, Master of Computer Applications in Mailam Engineering College from Anna University and also Master of Technology respectively from Bharathidasan University, India. I had one year Industrial Experience, presently I am working as an Assistant professor in Department of Computer Applications at Shanmuga Industries Arts and Science College, Tiruvannamalai, TamilNadu, India. My research interests include Cloud Computing and Cloud based Security.

Ms..A.TamilSelvi M.Sc., M.Phil., B.Ed.,I am working as an Asistant Professor in Department of Computer Science, Aruna Vidhya Arts and Science College, Kannakurukkai, Tiruvannamalai, TamilNadu, India. My Research is Network Security and DBMS. I really proud to do this paper as Research Journal.