IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Digital Watermarking to Insert Multiple Watermarks Sequentialy

Anjali R.Mundhe*1, Sneha M.Narhare[2], Prema B.Saudagar[3], Prof.D.V.Biradar[4]

*1,2,3,4 Department of Information Technology, M.S.Bidve engg.college, Latur, Maharashtra, India

dhanashritorgalkar@gmail.com

Abstract

Watermark is nothing but the data embedding and information hiding. we can simply say that digital watermarking is a pattern of bits inserted into a digital image, audio or video file which helps to identify the copyright information i.e. author, rights etc. In another way it is the method of embedding data into digital multimedia content. This is used to verify the credibility of the content or to recognize the identity of the digital content's owner.

In our project work we are going to insert the multiple watermarks in images. The watermark is embedded implicitly by determining multiple desired constraints of feasible image. These constraints ensures that the watermarked image is visually indistinguishable from the original one.

Keywords: .

Introduction

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking can be considered as a special technique of steganography where one message is embedded in another and the two messages are related to each other in some way. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low-energy signal is called watermark. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. An entity called watermark key used for embedding and detecting watermark signal.Watermark key is private.[2][7]

Characteristics of Digital Watermarking

- Invisibility**:** an embedded watermark is not visible.
- Robustness: piracy attack or image processing should not affect the embedded watermark.
- Readability: A watermark should convey as much information as possible. A watermark should be statistically undetectable. Moreover, retrieval of the digital watermark can be used to identify the ownership and copyright unambiguously.
- Security: A watermark should be secret and must be undetectable by an unauthorized user in general. A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. As information security techniques, the details of a digital watermark algorithm must be published to everyone. The owner of the intellectual property image is the only one who holds the private secret keys.

The watermarking is classified in following ways

a) Robust & Fragile Watermarking
b) Visible & Invisible Watermarking
c) Public & Private Watermarking

a)Robust & Fragile watermarking- Robust watermarking is a watermarking if there is any modification in original data then there is no change in watermark whereas fragile watermarking means if there is any change om original data the watermark will change.

b) Visible & Invisible Watermarking- Visible Watermarking is visual to human eye whereas Invisible Watermarking is unvisible to human eye.[3][5]

c)Public & Private Watermarking- Public watermark does not require the original data to recover the watermark information but private watermark requires the original data to recover the watermark information.

Digital watermarking works in 3 parts
1)watermark insertion
2)watermark extraction
3)watermark detection

A Generic watermarking system :

When a user receives an image, he uses the detector to evaluate the authenticity of the received image. The detection process may require knowledge of the marking key, the watermark and the original image.The detector is usually based on statistical detection theory whereby a test statistic is generated and from that test statistic the image is determined to be authentic. If it is not authentic then it would be desirable for the detector to determine where the image has been modified.[10]

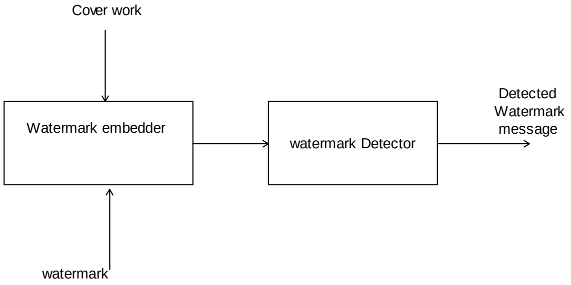

Fig.1Watermark insertion:

A user wants to insert the watermark into the image at that time he uses a key that may be public or private .this key is used for authencity purpose.the input for this process is key,input image and watermark.

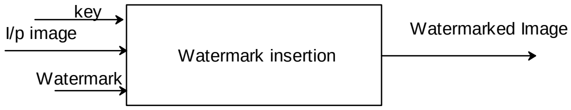

Fig.2 Watermark Extraction:

Extraction is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. Inputs to the scheme are the watermarked data, the secret or public key and, depending on the method, the original data and/or the original watermark. The output is the recovered watermarked W or some kind of confidence measure indicating how likely it is for the given watermark at the input to be present in the data under inspection.

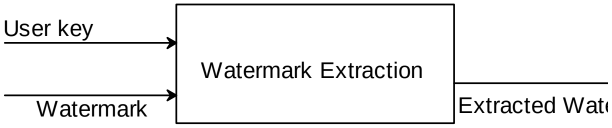

Fig.3 Flow of Watermark Extraction:

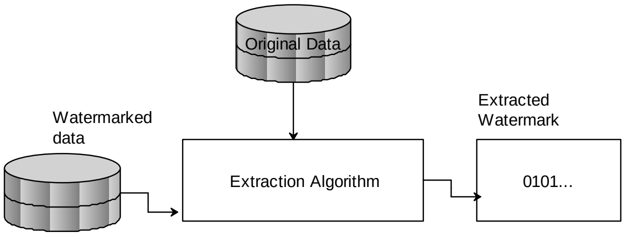

Fig.4 Diagram for Watermark Detection:

The fig. shows that whether the watermark is inserted or not .To check this we use the key (may be private or public)and watermark image with specific id . on this basis The detection algorithm detects that whether it contains watermark or not .if it is detected then it gives answer yes otherwise no.

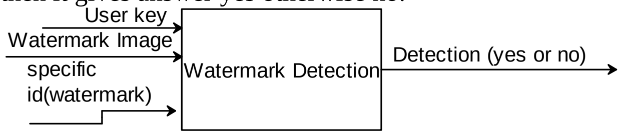

Fig.5 Structure of Watermark Embedding process:

In embedding, an algorithm accepts the data to be embedded, and using watermark it produces a watermarked signal. Inputs to the scheme are the watermark, the original data and an optional public or secret key(not mandatory). The outputs are watermarked data. The key is used to enforce security.

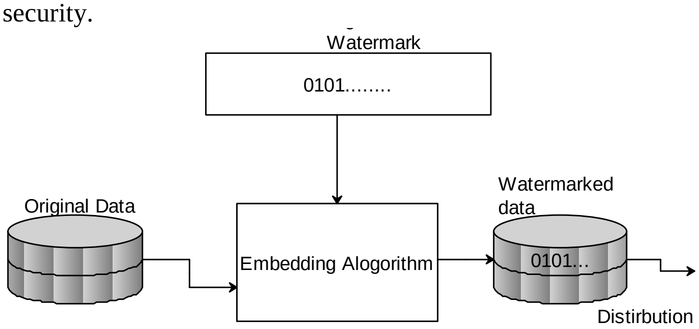

Fig.6

Applications of Watermarking

- Security

In the field of data security, watermarks may be used for certification, authentication, and conditional access.

Certification

It is an important issue for official documents, such as identity cards or passports. Digital watermarking allows to mutually link information on the documents. That means some information is written twice on the document, for instance, the name of a passport owner is normally printed in clear text and is also hidden as an invisible watermark in the photo of the owner. If anyone would intend to duplicate the passport by replacing the photo, it would be possible to detect the change by scanning the passport and verifying the name hidden in the photo does not match any more the name printed on the passport.

Authentication

The goal of this application is to detect alterations and modifications in an image. Suppose we have picture of a car that has been protected with a watermarking technology. And if, the same picture is shown but with a small modification, say, the numbers on the license plate has been changed. Then after running the watermark detection program on the tampered photo, the tampered areas will be indicated in different color and we can clearly say that the detected area corresponds to the modifications applied to the original photo.

Conditional Access

For example conditional access to confidential data on CD-ROMs may be provided using digital watermarking technology. The concept consists of inserting a watermark into the CD label. In order to read and decrypt the data stored on the CD, the watermark has to be read since it contains information needed for decryption. If someone copies the CD, he will not be able to read the data in clear-text since he does not have the required watermark.

- Copyright Protection

Copyright protection inserts copyright information into the digital object without the loss of quality. Whenever the copyright of a digital object is in question, this information is extracted to identify the rightful owner. It is also possible to encode the identity of the original buyer along with the identity of the copyright holder, which allows tracing of any unauthorized copies.

- Other applications

Digital watermarks can also serve as invisible labels and content links. For example, photo development laboratories may insert a watermark into the picture to link the print to its negative. This way is very simple to find the negative for a given print. All one has to do is scan the print and extracted the information about the negative. In order to distinguish between different copies, different watermarks are embedded into different copies of the same document. These marks are also called "digital fingerprints".

Existing System

The existing digital watermarking methods are based on single water marking so that they provides less security to the image. Although some researchers focused on the viability of existing watermarking approaches for the insertion of multiple signatures, the development of specific techniques can provide much more effective results. The general problem of multiple digital watermarking has been the object of several investigations since the pioneering contribution. It is suggested that the insertion of multiple watermarks can be exploited to convey multiple sets of information. More recently, a multiple watermark-embedding procedure was proposed, which allows simultaneous insertions without requiring the key sets to be orthogonal to each other. Specific applications such as the already mentioned medical image management may even require the insertion of two different types of watermark, namely, a robust one for authentication purposes, and a fragile one for data integrity control. This paradigm is often referred to as multipurpose watermarking.[6][7][8]

Proposed System

In our dissertation work, we are introducing a new concept which allows that tracing and sharing of property of image documents to embed multiple watermarks sequentially into the data.The insertion and detection of watermark is performed on digital image.The main part of this work allows us to insert multiple watermarks by more than one user in sequential manner which does not require any extra information besides the public keys. This approach improves the quality of present available techinque. The main advantage of this approach is, it solves the problem affecting other recent approaches where each user needs to know the secret keys used to embed all previous watermarks to successfully insert his signature.[9]

The dissertation work, based on elementary linear algebra, is asymmetric, which involves private key to embed the watermark and a public key to detect the watermark. 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 applications refer to a collaborative environment, in which malicious attacks are not a critical aspect.[1][9]

We are implemented here a watermarking scheme, which allows to insert and reliably detect multiple watermarks sequentially embedded into a digital image, as it is a challenging task in Digital Image Processing.[3]

Conclusion

The dissertation work , allows to insert and reliably detect multiple watermarks sequentially embedded into a digital image, as it is required by challenging Digital Right Management applications such as confidential data tracing and shared property handling.

The proposed method is based on elementary linear algebra which is asymmetric, this involves a private key for embedding and a public key for detection. it is robust and more secure to avoid malicious attacks.

References

[1] *Giulia Boato, Member, IEEE,Francesco G. B. De Natale, Senior Member, IEEE, and Claudio Fontanari*

[2] *Oktay Altun, Gaurav Sharma and Mark Bo cko ECE Department,University Of Rochester, Rochester, NY, 14627*

[3] *Boato, G. Dept. of Inf. & Commun. Technol., TreDe Natale, F.G.B.; Fontanari, C. "Multimedia, IEEE Transactions on digital Image Watermarking", Volume: 9 , Issue: 4 Page(s):677 - 686 Product Type: Journals & Magazines,June 2007.*

[4] *G. Coatrieux , H. Maitre , B. Sankur , Y. Rolland and R. Collorec "Relevance of watermarking in medical imaging", Proc. IEEE EMBS Int. Conf. Information Technology Applications in Biomedicine 2000, pp.250 -255 2000*

[5] *A. Giakoumaki , S. Pavlopoulos and D. Koutsouris "Multiple image watermaking applied to health information management", IEEE Trans. Inf. Technol. Biomed., vol. 10, no. 4, pp.722 -732 2006*

[6] *F. Mintzer and G. W. Braudaway "If one watermark is good, are more better?", Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 1999, vol. 4, pp.2067 -2069 1999*

[7] *C.-T. Hsu and J.-L. Wu "Hidden digital watermarks in images", IEEE Trans. Image Process., vol. 8, no. 1, pp.58 -68 1999*

[8] *P. H. W. Wong , O. C. Au and Y. M. Yeung "A novel blind multiple watermarking technique for images", IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp.813 -830 2003*

[9] *P. H. W. Wong , A. Chang and O. C. Au "A sequential multiple watermarks embedding technique", Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 2004, vol.3, pp.393 -396 2004*

[10] *Watermarking techniques for alternative requirements By Teddy Furon*