Research Paper Engineering

Digital Watermarking for Image Processing

*Anil P .Gaikwad ** Bhagyashri R. More

*, ** Professor, PDVVPF's IBMRD, Vilad Ghat, Ahmednagar

ABSTRACT

Now a day's digital data is most commonly spread on the internet due to the rapid development of internet. Now the question arise is how protect our important data from being stolen or modified has become an important issue. For this, Digital watermarking is one of the solutions which can protect digital rights by embedding owner watermarks into the digital data, so the owner can declaim his ownership and intellectual property. This paper presents how digital watermarking techniques work to protect our digital data.

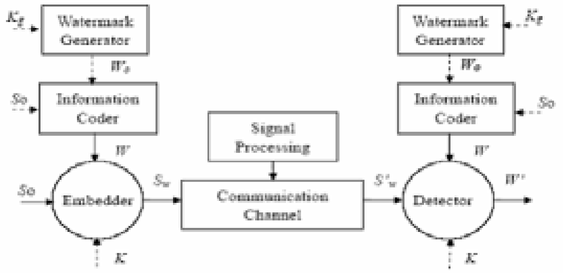
Introduction:

What is Watermark?

v Watermark-an invisible signature embedded inside an image to show authenticity or proof of ownership

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, atop a dark background), caused by thickness or density variations in the paper.

- Watermarking-The process of embedding information into another object.



Diag1: General Watermarking System

- **Digital Watermarking-**

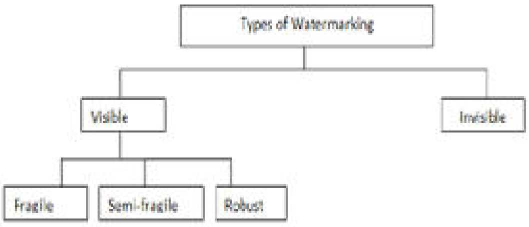
Digital watermarking is the technologies that allow hiding of essential data or information in digital media, such as images, video and audio. Watermarking techniques embed information in images by introducing changes that are hardly noticeable to the human eye but recoverable by a computer program.

- It helps to protect from unauthorized copying and distribution of images over the internet
- Ensure a digital picture has not been altered
- Various Software can be used to search for a specific watermark

- **procedure of watermarking**

1. Generating & Processing a Key/Data
2. Generating & Embedding watermark
3. Constructing a Proof
4. Verifying a Proof

Digital watermarking can be divided into two types, that are-visible and invisible.

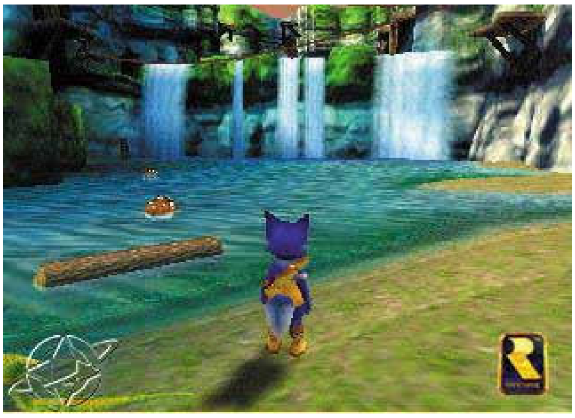


Diag 2: Types of watermarking

Visible Watermark:-The visible watermarks are viewable to the normal eye such as bills, company logos and television channel logos etc. This type of watermarks is easily viewable without any mathematical calculation but these embedded watermarks can be destroyed easily.

- Fragile: A watermark is said to be fragile if the watermark hidden within the host signal is destroyed as soon as the watermarked signal undergoes any manipulation.
- Semi-Fragile: Signal modification is sensitive in semi fragile. It is feature of both robust and fragile watermark. It helps to provide authentication
- Robust: It embedded in invisible watermark. It resists image attacks. It helps to protect or verify ownership

Example of Visible Watermark



Diag 3: Example of Visible Watermark

Invisible Watermark:-The invisible watermarks, the locations in which the watermark is embedded are confidential; only the authorized persons can fetch the watermark. Some mathematical calculations are required to retrieve the watermark. This kind of watermarks is not viewable by an ordinary eye. Invisible watermarks are more secure and robust than visible watermarks.

Example of Invisible watermark

Watermarks: Secret Code for Protection
1
2
3

Diag 4: Example of Invisible watermark

Properties of Digital Watermark

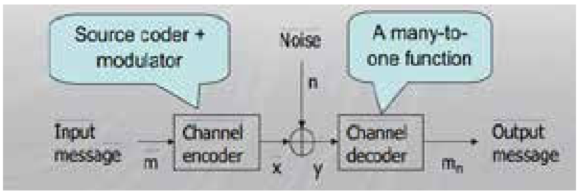
- Perceptually invisible
- Robustness
- Cost
- Capacity
- Recoverable
- Reversible
- Undetectable
- Able to determine the true owner
- High bit rate

Models of Watermarking:

1. Communication-based models of watermarking
2. Geometric models of watermarking
3. Modeling watermark detection by correlation

1.Communication-based models of watermarking-
In this watermarking is vies as a transmission channel through which watermark message is communicated.

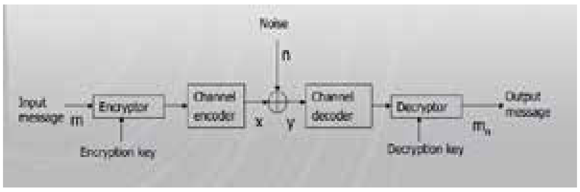
Components of Communication Systems



Diag 5: Components of Communication Systems

- m: the message we want to transmit
- x: the codeword encoded by the channel encoder
- n: the additive random noise
- y: the received signal

Secure Transmission:



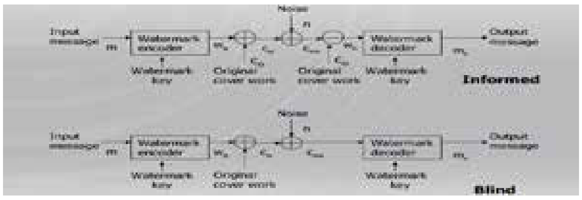
Diag 6: Secure Transmission

Cryptography

- Prior to transmission, cryptography is used to encrypt a message using a key.
- The encrypted message (ciphertext) is transmitted over the channel
- At the receiver, the ciphertext is received and decrypted using the related key to reveal the cleartext

- Spread Spectrum Communication
  - Against signal jamming
  - Modulation is done according to a secret code, which spreads the signal over a wider bandwidth than required.

Watermarking As Communication Systems



Diag 7: Watermarking As Communication Systems

2. Geometric models of watermarking-
Distribution of unwatermarked Works

- Describing how likely each Work is
- Region of acceptable fidelity
  - A region in which all Works appear essentially identical to a given cover Work
- Detection region
  - Describing the behavior of the detection algorithm
- Embedding distribution/region
  - Describing the effects of an embedding algorithm
- Distortion region
  - Indicating how Works are likely to be distorted during normal usage

3. Modeling watermark detection by correlation:
There are several types of watermark detection by correlation like linear correlation, normalized correlation and correlation coefficient.

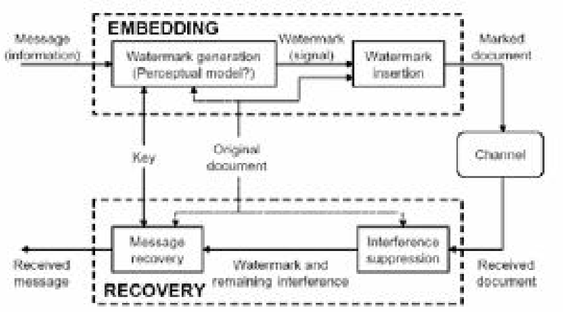
- **Watermark Mechanism:**

undeniable watermark- notation : image

{W1,W2,^ ,Wn}:watermark
W : watermarked image
E : encoder
D : decoder

D(I ‘, I) = P(W), P : indicating function of presence of wm F (I) = { f1 (I), f2 (I),Λ , fn (I)} : derived feature

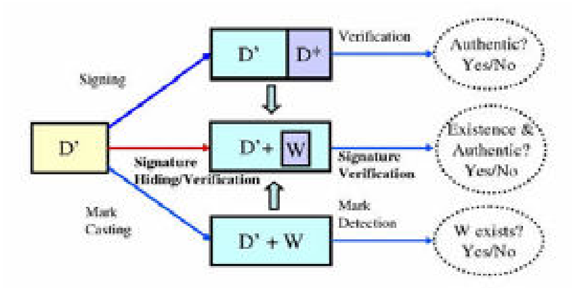
- **overall embedding and recovery mechanisms**



Diag 8: Digital watermark module

- **Watermark Verification**
  - GEN_KEY
  - asymmetric watermarking scheme
  - symmetric watermarking scheme
  - un-keyed watermarking scheme
  - GEN_W
  - E
  - D
  - D(I ‘, W , I, kdet)

Informed detection vs. blind detection
three watermarking mechanisms for digital data D'



Diag 9: Watermark verification and authentication mechanism

- **Attacks on Digital Watermarking**
  - How we can identify the original watermark?
  - How can we identify which watermarked version of an image is the truly watermarked version in circulation?
  - Lossy Compression
  - Geometric Distortions
  - Common Signal Processing Operations
    - Linear filtering such as high pass and low pass filtering
    - Non-linear filtering such as median filtering
    - Addition of a constant offset to the pixel values
    - Addition of Gaussian and Non Gaussian noise
    - Local exchange of pixels
  - Jitter Attack
  - How we can suggest the concrete protocol

- **Watermarking Techniques:**
  - Spatial Domain Watermarking-embedded by modifying pixel value. Spread spectrum approach
  - Transform Domain watermarking-Embedded in transform domain like Wavelet

- **Applications of image watermarking :**
  - IPR Protection
  - Demonstration of rightful ownership
  - Authentication
  - Labeling for data retrieval
  - Covert communication

Conclusion:
Watermarking help us to find solutions for problems regarding digital data, as we regard it as the designated verification process. If there are multiple watermarked images, the original owner can cooperate with its verification process. Now our challenge is to focus on issues such as image resampling and image rotation for further.

REFERENCES

1.M. Kutter, F. Hartung, "Introduction to Watermarking Techniques" in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 97-119 | 2. C.-T Hsu and J.-L. Wu, "Multiresolution watermarking for digital images," IEEE Trans. Circuits Syst. II, vol. 45, pp. 1097–1101, Aug 1998. | 3. Digitized [electronic resource] : the science of computers and how it shapes our world / Peter J. Bentley. | Website: | http://www.inspirenignite.com | www.google.com | www.wikepedia.com |