Fragile Watermarking Scheme for Image Authentication

Source: Electronics Letters, Vol. 39, No. 12, June 2003, pp. 898-900

Authors: Hongtao Lu, Ruiming Shen, and Fu-Lai Chung

Speaker: Wen-Chuan Wu

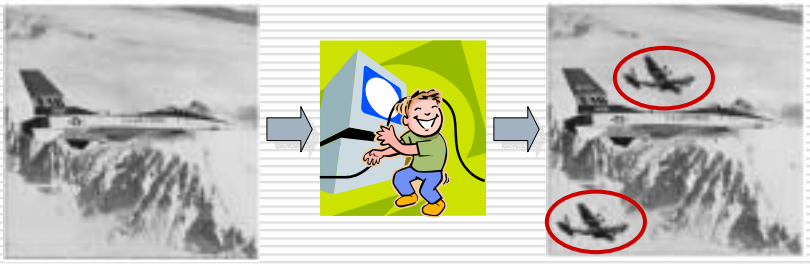
Date: 2005/03/24

Outline

- Fragile watermarking
- Wong's scheme
- The proposed scheme
  - Watermark embedding
  - Watermark extraction
  - Tamper Detection
- Experimental results
- Conclusions

Introduction

- Watermarking scheme
  - Robust: copyright, ownership verification.
  - Fragile: authentication and integrity.

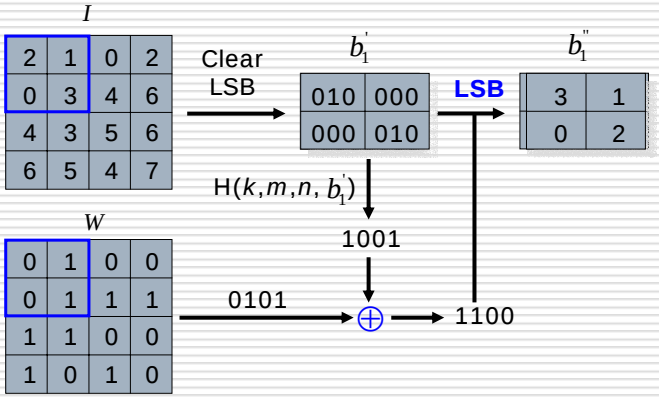


Sender Receiver

Previous work (Wong's scheme)

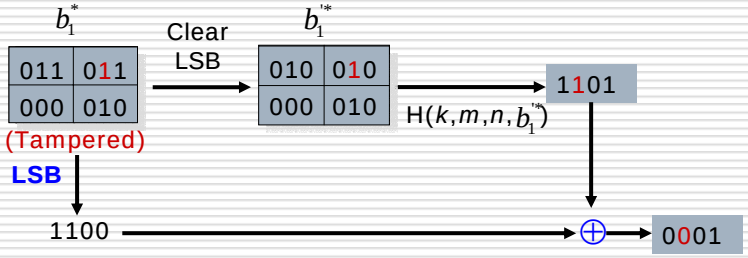
- Embedding

L =[0,1,2,3,4,5,6,7]



k: secret key

Verification

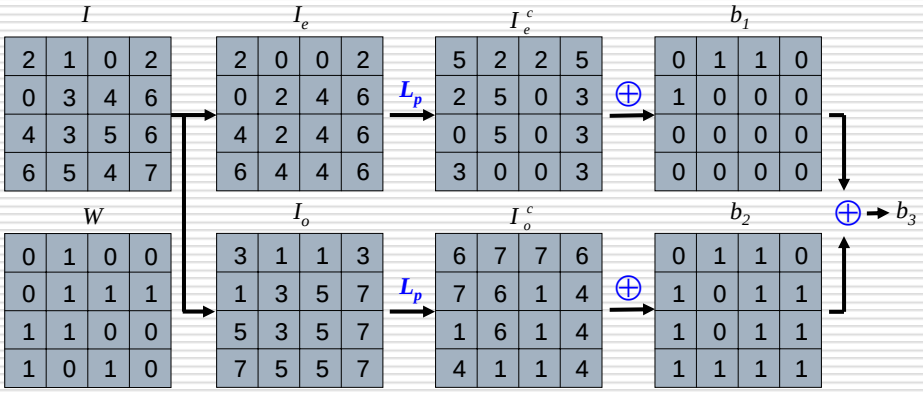


Drawback: suffer from The VQ attack

Proposed scheme

Embedding

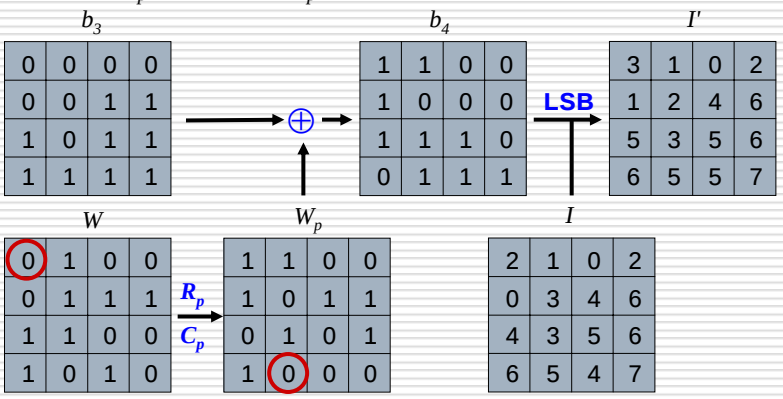
L =[0,1,2,3,4,5,6,7]
L_p=[2,7,5,6,0,1,3,4]



Proposed scheme (Con't)

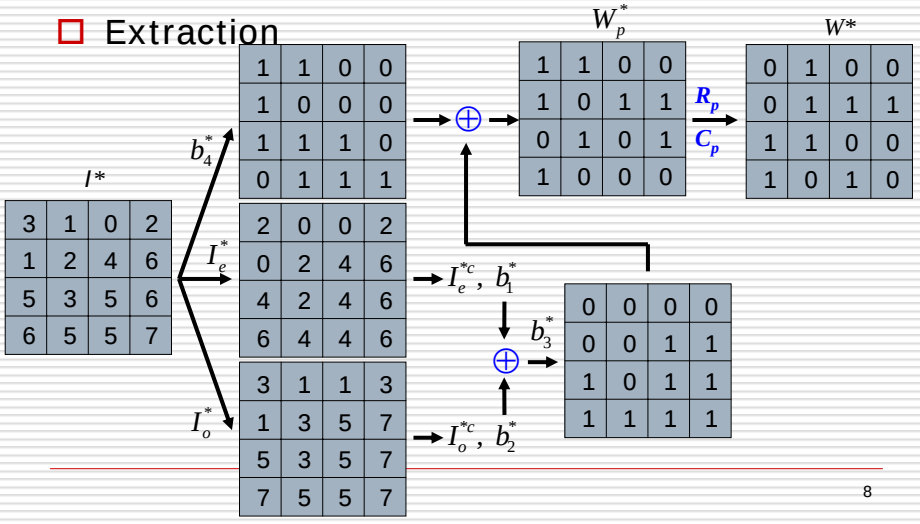
R =[1,2,3,4] ; C =[1,2,3,4]

R_p=[4,2,1,3] ; C_p =[2,1,4,3]



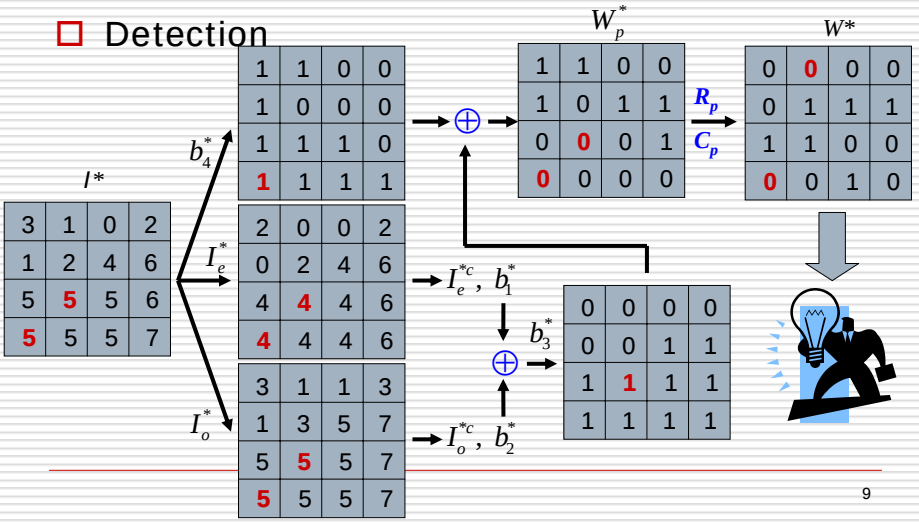
Proposed scheme (Con't)

- Extraction

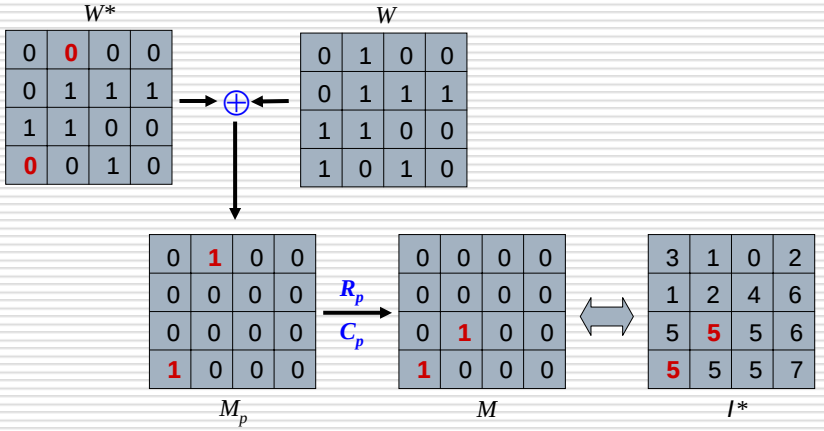


Proposed scheme (Con't)

- Detection

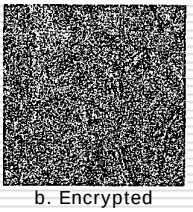


Proposed scheme (Con't)



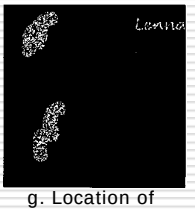
Experiments

a. Original image (8-bit)



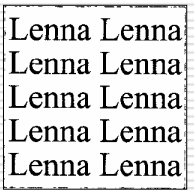
b. Encrypted image

e. Modified image

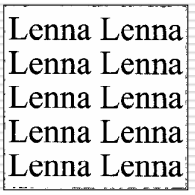


g. Location of modified area

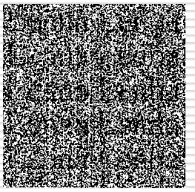
c. Watermarked image



d. Extracted watermark from c



f. Extracted watermark from e



h. Extracted using wrong key

Conclusions

- The original host image is not needed in the extraction phase.
- It is based on random permutation of both the host image and the watermark.
- It is a pixel-based fragile watermarking method, so avoids the VQ attack.