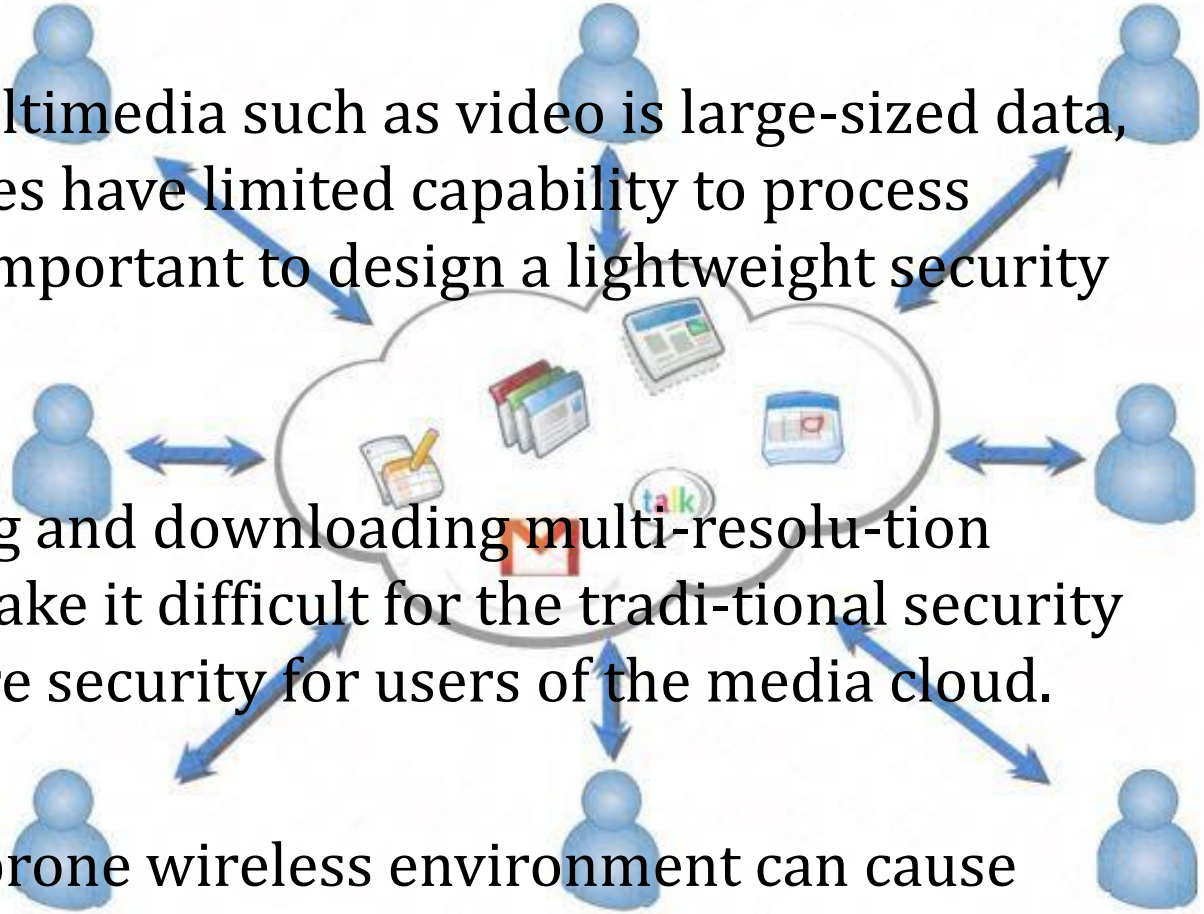
Security Protection between Users and the Mobile Media Cloud

Honggang Wang, University of Massachusetts
Shaoen Wu, Ball State University
Min Chen, Huazhong University of Science and Technology
Wei Wang, South Dakota State University

資工二乙 劉源葦

２０１４／５／８

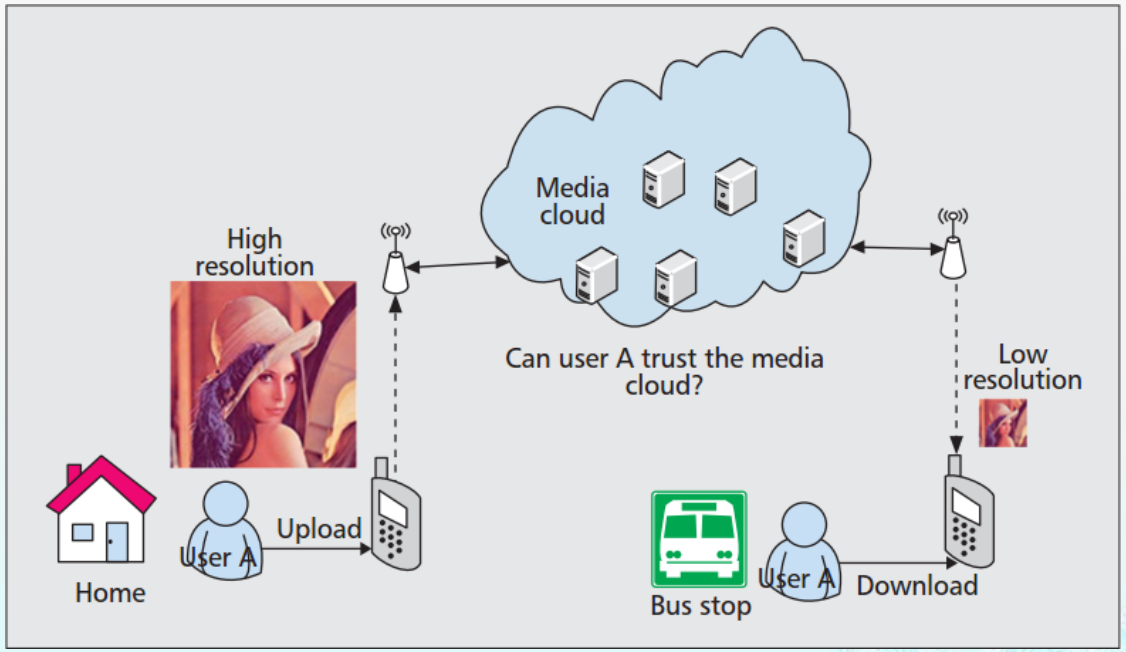
INTRODUCTION



- First, because multimedia such as video is large-sized data, and mobile devices have limited capability to process media data, it is important to design a lightweight security method;
- Second, uploading and downloading multi-resolu-tion images/videos make it difficult for the tradi-tional security methods to ensure security for users of the media cloud.
- Third, the error-prone wireless environment can cause failure of security protection such as authentication.

INTRODUCTION

- A critical question must be answered when the mobile clients upload their multimedia to the cloud: can users trust the media cloud?

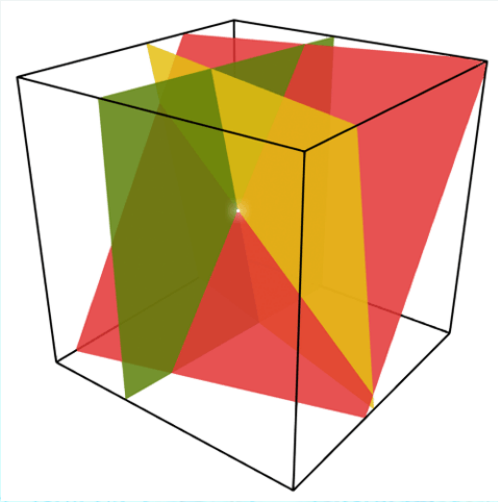


RELATED WORKS

- First, the embedded watermark should not degrade the quality of the image and should be perceptually invisible to users in order to maintain its protective secrecy.
- Second, the watermark must be robust enough and not easily removable.
- Third, the blind watermarking technique has to be adopted since sometimes it is not easy to obtain the original image or original watermark during extraction.

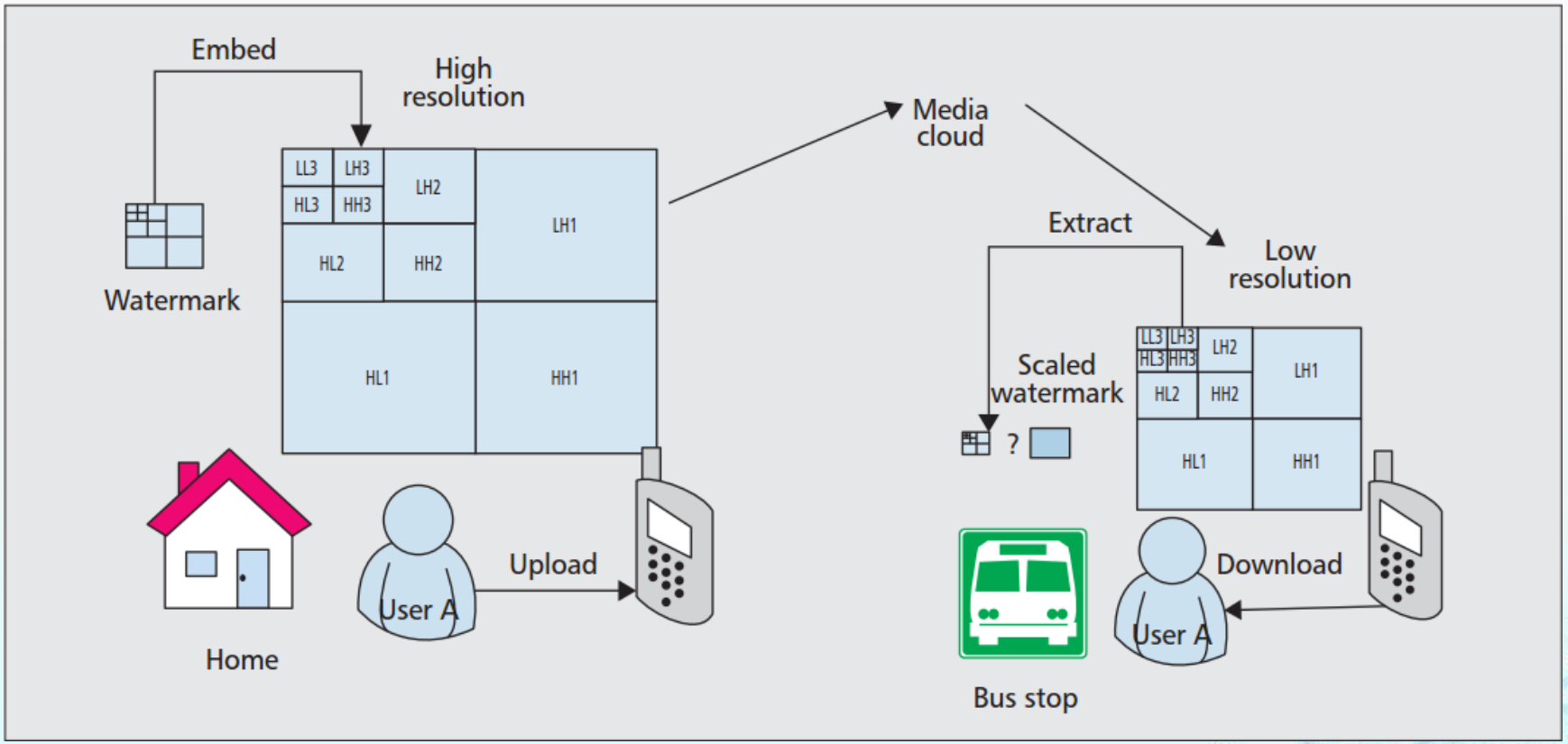
RELATED WORKS

- Some techniques such as image hiding to increase the security of the image have also been proposed.
- However, the common weakness of these techniques is that the image data are all in a single information carrier.
- Shamir et al. independently proposed the concept of secret sharing called the (r,n) threshold scheme.



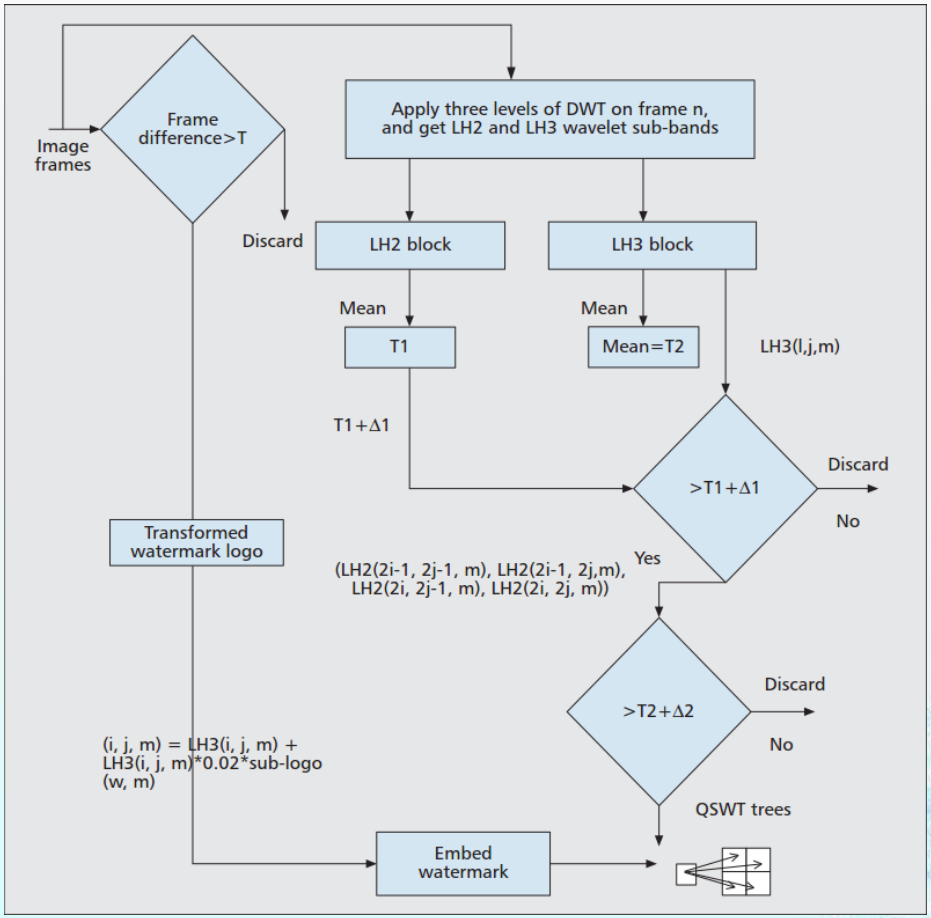
In this article, we propose DCT-based secret sharing for protecting users' data to the media cloud.

The proposed watermark embedding algorithm



SCALABLE WATERMARKING FOR THE MEDIA CLOUD

- Our proposed watermark embedding algorithm based on QSWT is described



Discrete wavelets transform (DWT)

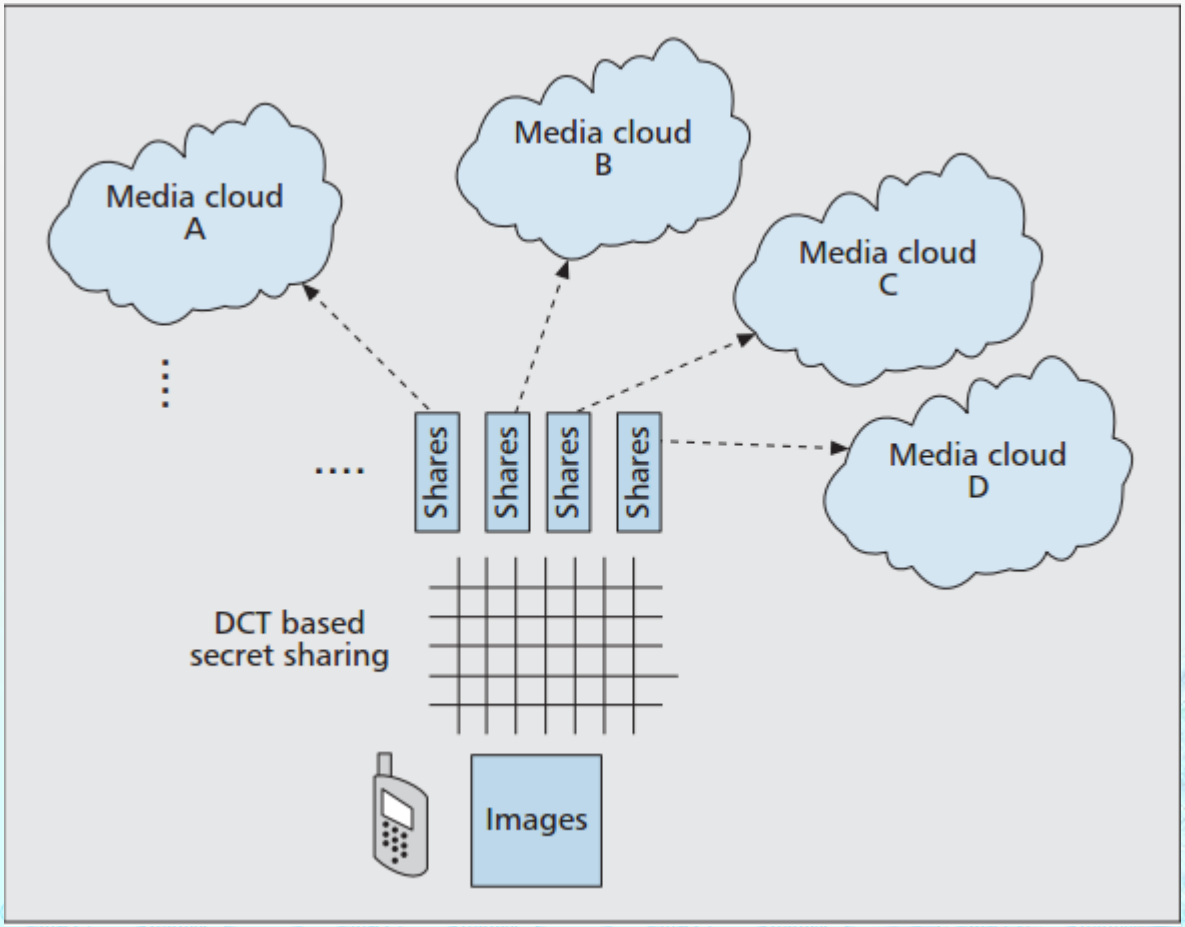
JOINT DESIGN OF WATERMARK AUTHENTICATION AND ERROR CORRECTION CODES FOR MEDIA CLOUD

- While there are several forward error correction (FEC) techniques available, Reed-Solomon (RS) codes provide powerful correction with high channel efficiency.

- For the joint design of RS and watermarking, two approaches have been considered.
  - In the first method, the full watermarked image is given as input to an RS encoder.
  - In the second method, only the LH3 band is given as input to the RS encoder.

SECRET SHARING FOR MEDIA CLOUD

- We use a low-complexity DCT-JPEG-based compression algorithm for mobile media cloud so that the transmission load can be effectively reduced.



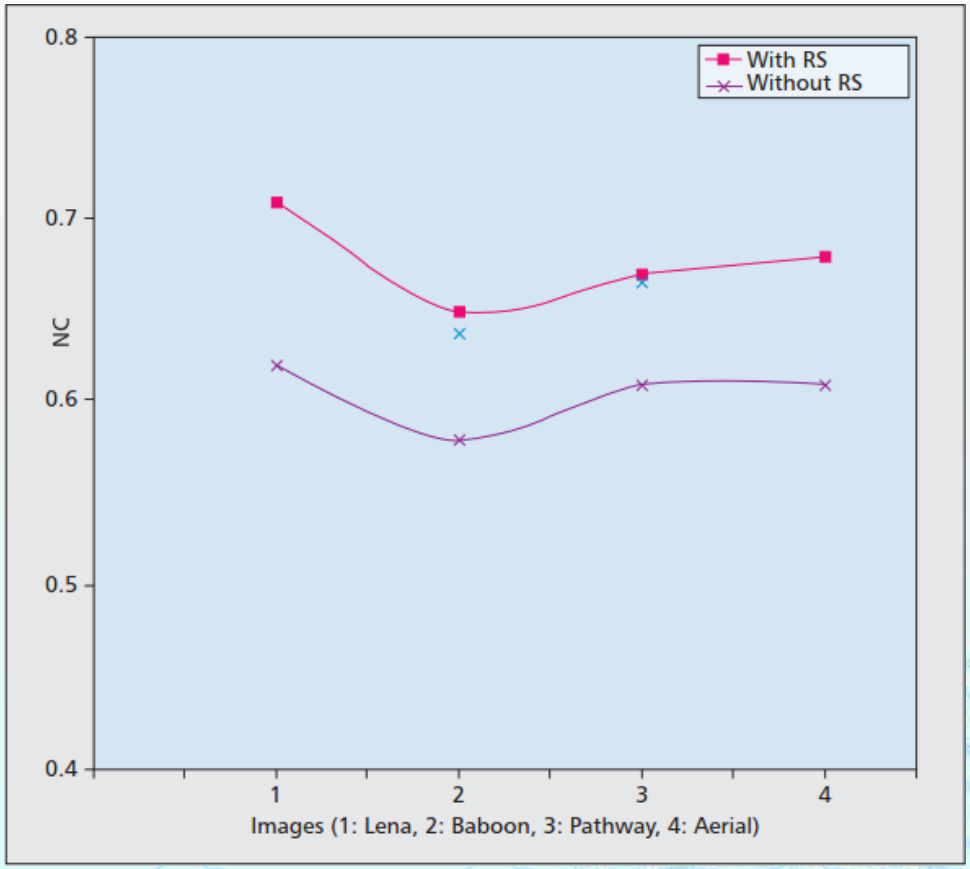
With noise and Reed-Solomon code

- We evaluated our approach on different types of images.

Images	Noise density 0.05			Noise density 0.15			Noise density 0.45		
	PSNR	NC	#(Ex)	PSNR	NC	#(Ex)	PSNR	NC	#(Ex)
Lena	27.85	0.71	1825	20.57	0.66	1686	19.59	0.64	1650
Baboon	27.65	0.66	1682	20.68	0.62	1573	19.63	0.59	1527
Pathway	27.53	0.68	1728	20.41	0.64	1613	19.23	0.62	1581
Aerial	27.05	0.68	1751	20.35	0.63	1624	19.04	0.62	1614

Normalized correlation

- We conclude that the joint design of watermark and RS code can achieve better authentication performance.



CONCLUSION

- In this article, we present a joint design of watermarking technique based on the significant difference of wavelet quantization with the Reed-Solomon error correcting code.
- The watermarking technique authenticates multimedia data from the media cloud, and the Reed-Solomon code guarantees that data trans-mission is reliable for multimedia data between mobile users and the media cloud.
- In addition, we propose the use of secret sharing schemes to maintain users' data security and privacy.