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

ABSTRACT

Mobile devices such as smartphones are widely deployed in the world, and many people use them to download/upload media such as video and pictures to remote servers. On the other hand, a mobile device has limited resources, and some media processing tasks must be migrated to the media cloud for further processing. However, a significant question is, can mobile users trust the media services provided by the media cloud service providers? Many traditional security approaches are proposed to secure the data exchange between mobile users and the media cloud. However, 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-resolution images/videos make it difficult for the traditional 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. To address the above challenges, in this article, we propose to use both secure sharing and watermarking schemes to protect users' data in the media cloud. The secure sharing scheme allows users to upload multiple data pieces to different clouds, making it impossible to derive the whole information from any one cloud. In addition, the proposed scalable watermarking algorithm can be used for authentications between personal mobile users and the media cloud. Furthermore, we introduce a new solution to resist multimedia transmission errors through a joint design of watermarking and Reed-Solomon codes. Our studies show that the proposed approach not only achieves good security performance, but also can enhance media quality and reduce transmission overhead.

INTRODUCTION

With the fast development of current information technology, electronic publishing, such as the distribution of digitized images and videos, is becoming more and more popular. Digital multimedia content such as images and videos can easily be sent through the Internet to the cloud system. In particular, data access over wireless networks from the media cloud has recently found increased popularity due to the fast growth of wireless multimedia applications. However, multimedia security has become an increasingly major concern for cloud media data access control. It is important to ensure secure and reliable multimedia data transmissions between mobile users and the media cloud.

Since the data can be transferred and stored in a cloud system through wireless, it becomes vulnerable to unauthorized disclosures, modifications, and replay attacks. A critical question must be answered when the mobile clients upload their multimedia to the cloud: can users trust the media cloud?

As shown in Fig. 1, user A uploads his/her image to the media cloud when he/she is at home using the mobile phone. Later on, he/she wants to access the same media (e.g., an image) from the media cloud when he/she is at a bus stop. The question is how to assure user A that the media data has not been modified by others.

It is reasonable that a cloud system can provide security access control. However, the cloud itself may not be trusted since it is managed by third parties such as cloud service providers. The security can only be guaranteed by contracts between users and cloud service providers. There are some potential risks, such as security attacks or misconduct of the cloud manager. Strictly speaking, users should only trust themselves rather than cloud security services. A further question is, can users have other approaches to protect their media data from the media cloud? In this article, we propose to utilize secret sharing and watermarking to address the challenges. Our design is user-oriented, and allows users to protect their data's security and privacy. First, we focus our studies on media authentication. It is well known that some steaming level authentication methods such as media authentication

 0163-6804/14/$25.00

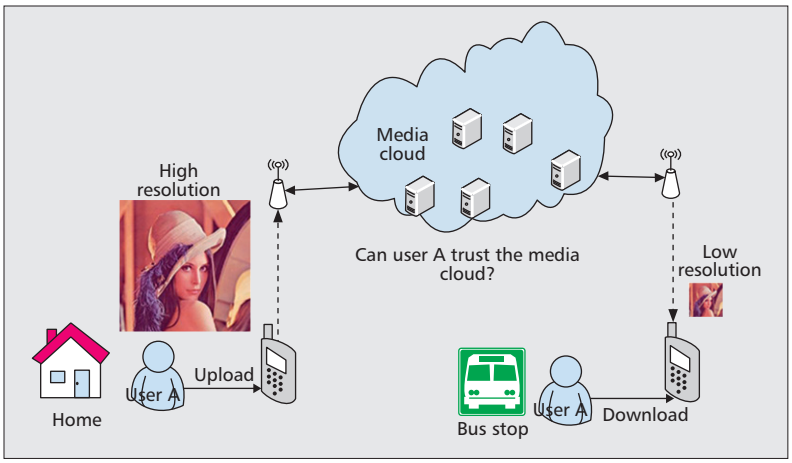

Figure 1. *Can user A trust the media cloud?*

code (MAC) or content level approaches such as watermarking can be used to authenticate media data over wireless networks.

However, MAC approaches generate high overhead due to adding hash values to each media packet. Content-level authentication approaches such as watermarking consider the characteristics of media data and thus can be used to authenticate media with lower overheads. However, both traditional streaming-based authentication and content level approaches fail to deal with the authentication of scaled multimedia over wireless networks. As shown in Fig. 1, user A uploads a large high-resolution image at home using WiFi to the media cloud for storage. When the user moves to a bus stop, he/she might want to download the image at lower resolution due to limited bandwidth and battery resource. In the scenario, it is worth noting that the user needs to guarantee the media integrity by themselves. If we use traditional watermarking algorithms, the watermark may not be detectable due to the image's compression and scaling to a smaller size. Therefore, a key issue is how to verify that the downloaded multimedia is not modified in the cloud. Traditional packet level authentication approaches are not feasible to deal with this problem. In this article, we propose a scalable authentication approach using watermarking, which could be scalable and adapted to the size of a scaled image from the media cloud. Another research challenge in the article is the reduction of wireless transmission errors, which could corrupt the embedded watermark and fail the process of watermark detections.

Furthermore, we propose using a secret sharing scheme to divide multimedia data into multiple pieces and then uploading them to different clouds. In this situation, even the data pieces in one cloud are disclosed, but all of the information cannot be disclosed due to the nature of secret sharing. The secret image sharing scheme is widely applied in visual cryptography. To secure an image, a secret image sharing scheme usually divides the image into n unreadable images (shares) with smaller size than the secret image. The secret image can be recovered by at least a threshold number (r) of shares known as the (r, n) secret sharing threshold.

On the other hand, scalable watermarking has become increasingly important for the online distribution of digital content. It allows content to be scaled for a wide range of users and devices under dynamic network bandwidth. Scalable compression allows different display resolutions and requires different bandwidth. However, for low-end devices, the scaling process may alter the embedded digital watermark. In the proposed watermark-based scalable authentication, users can embed scalable watermarks into digital images and upload them to the cloud. When the user wants to download their multimedia data back to their own devices, they just need to know partial content of the scalable watermark image and make some comparison to make sure the images are not corrupted or modified.

Related Works

In recent years, media cloud applications are growing with widely deployment of smartphones. A survey in media cloud is presented in [1] to overview trends in cloud mobile media (CMM) services, and opportunities and benefits for new CMM services. It is reported that developing scalable cloud media applications and cloud user experience measurement techniques are essential for future CMM. In [2], the authors present a novel concept of cloud-based mobile media service delivery, which is designed based on the localized media public cloud. The authors argue that the service quality is related to the location of the cloud. In [3], the authors focus on the studies of mobile cloud computing for multimedia applications. In [4], the authors conclude that mobile cloud computing can enable ubiquitous cloud mobile media (CMM) applications. One key issue for realizing the mobile media cloud application is concerns about data security and privacy. In the literature, the security issues within the cloud have been well studied and many solutions have been provided. However, there are only a few studies on the methods of securing the services between the mobile device and the cloud.

Multimedia has its own characteristics, and the traditional security methods for the mobile cloud have limitations such as higher computational and communication overhead. On the other hand, many researchers are aware of the issues of copyright protection, image authentication, proof of ownership, and so on. There are still several important research challenges for applying watermarking in the cloud. 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.

Several watermarking techniques were proposed in [5, 6] based on discrete cosine transform (DCT). Kwon *et al.* [7] embedded the

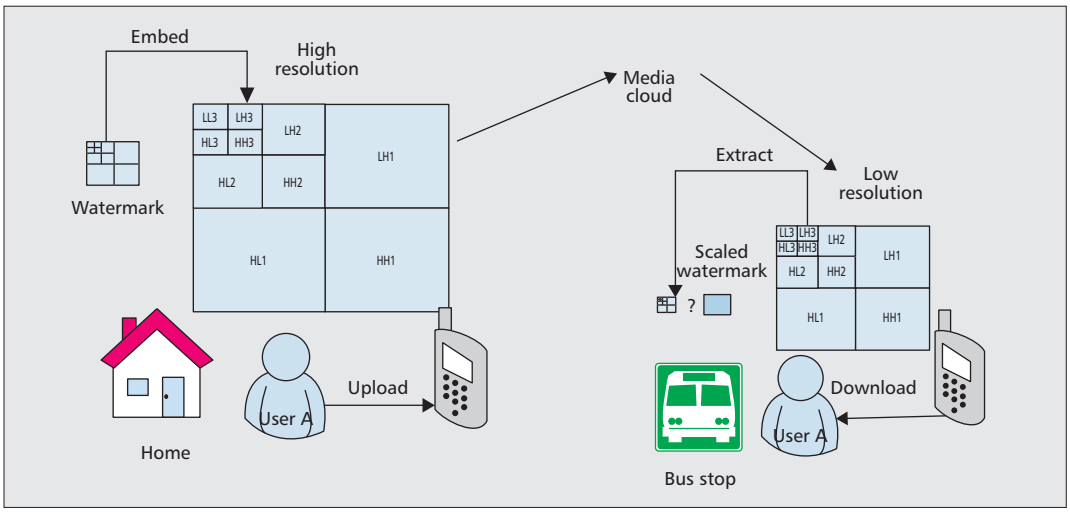

Figure 2. *The proposed watermark embedding algorithm.*

watermark in the variable DCT blocks. The DCT block size is determined according to the characteristics of the region in the spatial domain. Some watermarking methods were proposed based on the DWT [8]. In these methods, the watermark is embedded in the significant coefficient, which is selected from the wavelet coefficient. Huang and Yang [9] proposed a watermarking algorithm based on the DWT. The watermark is embedded into the wavelet coefficients in the middle and low subbands of a block of each image. A watermarking method based on the qualified significant wavelet tree (QSWT) was proposed in [10]. The issue of security in the multimedia cloud has become an major concern for data storage and access control over wireless networks. Reference [11] presents a strong user authentication framework for cloud computing, where users' legitimacy is strongly verified. The proposed framework provides multiple functions such as identity management, mutual authentication, and session key establishment between the users and the cloud server. A detail review of authentication in the clouds with its application to mobile users is presented in [12]. The mutual authentication between users and between user and end of cloud storage system is critical in ensuring data security. The research works related to security frameworks for wireless networks [13, 14] also contribute to the security between users and the media cloud.

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. The secret data cannot be revealed completely if the information carrier is lost or crippled. On the other hand, if we use many copies to overcome the weakness, the danger of security exposure will increase. Secret sharing schemes are based on the principle of sharing secret information among a group of players. Only when a coalition of willing players poll their shares together can secrets be recovered. In the proposed scheme, the secret image data may be disclosed only if a considerable number of image shares have been compromised.

The secret sharing approach proposed by Blakely would significantly increase transmission loads since each share has the same size for the source image data, which is not practical for mobile devices. Shamir *et al.* independently proposed the concept of secret sharing called the (r, n) threshold scheme. The succeeding studies were mainly related to security for key management. Because the number of bytes used in an image is usually very large, the utilization of a threshold scheme for multimedia would still waste many resources. Naor and Shamir extended the secret sharing concept into image research. The approach is not applicable for image transmissions and recovery for resource-limited mobile devices since the transmission load is significantly increased. An improved image secret sharing approach was presented by Thien and Lin . It significantly reduces the size of the image shares to $1/r$ of the original secret image (r is a bounded number of shares for information to be disclosed), and the secret images can be reconstructed conveniently. However, it requires that the image be permutated by a key before the image shares can be computed, which causes severe drawbacks and challenges to an image compression algorithm. In this article, we propose DCT-based secret sharing for protecting users' data to the media cloud.

Scalable Watermarking for the Media Cloud

The DWT-Based Watermarking Technique

Discrete wavelets transform (DWT)-based watermarking is within the category of frequency domain watermarking techniques. The process of transforming the image into its transform domain varies; hence, the resulting coefficients are different. Generally, the watermarked data are embedded in a transformed image. In other words, the watermark is inserted into transformed coefficients of the input image. Finally, inverse transform is performed on the watermarked image. The watermark detection process is the inverse procedure of the watermark insertion process.

Only when a coalition of willing players is polling their shares together, secrets can be recovered. In the proposed scheme, the secret image data may be disclosed only if a considerable number of image shares have been compromised.

The number of parity/redundant symbols that must be added to the message is determined by the amount of required capability of error corrections. The parity symbols must contain enough information to detect the values of the erroneous information symbols.

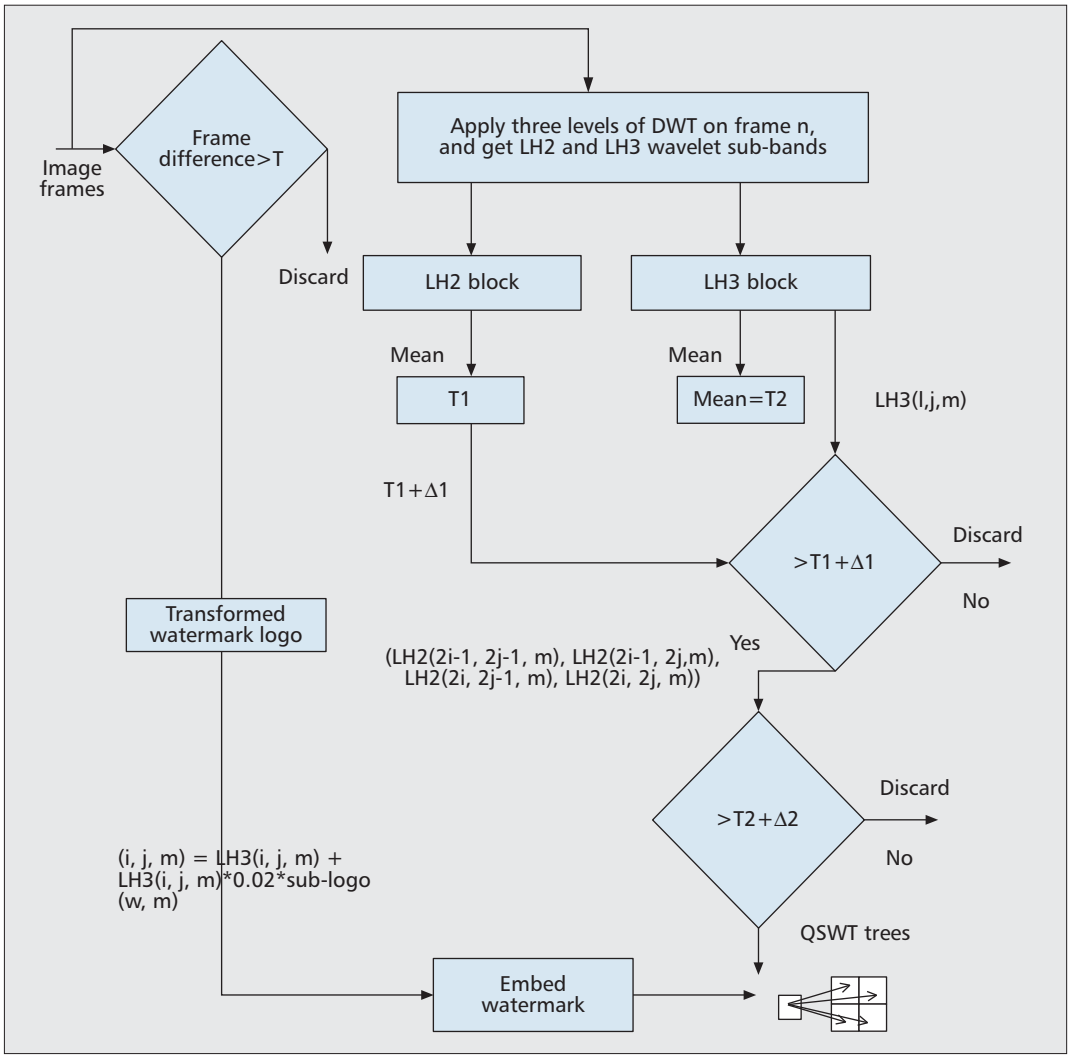

Figure 3. *The proposed watermark embedding algorithm.*

A blind watermarking algorithm based on a qualified significant wavelet tree (QSWT) is proposed by Lin *et al.* In this method, the image is transformed into wavelet coefficients using three-level DWT, and the LH3 subband is considered to embed the watermark as it is more significant than the HL3, HH3, and LL3 subbands. This technique is mainly based on the significant difference of wavelet coefficient quantization in which every seven non-overlapping wavelet coefficients of the host image are grouped into a block.

The Blind Watermarking Technique

Our proposed watermark embedding algorithm based on QSWT is described in Fig. 3. After a three-level DWT is applied in the input image frame n, wavelet subbands $LH2$ and $LH3$ are generated. The next step is to convert $LH2$ and $LH3$ to a set of smaller subblocks. T_1 and T_2 are acquired by calculating the mean of these subblocks in $LH3$ and $LH2$, respectively. For each coefficient at location $LH3(i, j, m)$ in subblock m, if it is greater than the threshold $T_1(m) + \Delta_1$, the system will check if at least three of its child coefficients ($LH1(2i - 1, 2j - 1, m)$, $LH1(2i - 1, 2j, m)$, $LH2(2i - 1, 2j - 1, m)$, and $LH2(2i, 2j, m)$ are greater than the threshold ($T_2(m) + \Delta 2$). If they are, $LH3(i, j)$ will be set as one of the QSWTs (m). The coefficient values of the parent and all its children are summed. Then QSWT (m) will be sorted in decreasing order, and these trees are output. All coefficients that do not meet these two adaptive thresholds are discarded. The original image is transformed using three-level DWT. From the 10 bands obtained, LH3 is used to embed the watermark. The watermark is embedded in the calculated QWST tree as described in [7].

Joint Design of Watermark Authentication and Error Correction Codes for Media Cloud

The number of parity/redundant symbols that must be added to the message is determined by the amount of required capability of error corrections. The parity symbols must contain enough information to detect the values of the erroneous information symbols. While there are several forward error correction (FEC) techniques available, Reed-Solomon (RS) codes provide powerful correction with high channel efficiency. With the advent of very large-scale

integration (VLSI) techniques, RS codes can be useful in both high and low data rate systems at low cost. The efficiency of RS codes is almost as the same as that of Hamming codes, except that RS codes deal with multibit symbols rather than individual bits. The main idea behind this work is to detect and extract the watermark data in which the watermarked data is subjected to noise caused by transmission. These noises might result in failure to detect watermarked data from the media cloud. The joint design mechanism could also extract more watermarking bits (higher robustness) than the general extraction algorithm. In the design, RS code plays an important role, extracting the watermarked bits, due to its ability to correct errors. 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. After the process of detecting and correcting errors, we replace the LH3 obtained from the RS code in the original image, and apply inverse DWT to reconstruct the image. In this scheme, packets are discarded if they cannot be corrected due to the bit errors caused by the noise. There is a trade-off between the quality and RS code protection in general. For example, having more RS protection will improve the quality with increased redundancy.

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. In the JPEG standard, each tile (i.e., every 8×8 pixel block) is converted to frequency space using a two-dimensional forward discrete cosine transform. Our secret sharing method is inspired by the (r, n) threshold scheme proposed by Shamir e*t al.* Specifically, we divide secret data Δ into n shadows $(\Delta_1, \ldots, \Delta_n)$, and the goal is that secret data Δ cannot be revealed without any r shadows. To split Δ into n shadows, a prime number p and an $r - 1^{\circ}$ polynomial function are selected,

$$f(x) = (a_0 + a_1 x \ldots + a_{r-1}x^{r-1}) \bmod P, \qquad (1)$$

where $a_0, a_1, \ldots, a_{r-1}$ are secret bits, and P is a larger prime number greater than any data values and can be made public. The shadows of the original secret data are

$$(\Delta_1 = f(1), \ldots, \Delta_i = f(i), \ldots, \Delta_n = f(n)).$$

In a secret image sharing scenario based on Shamir's (r, n) threshold scheme, a_0 is taken as the gray value of the first pixel, and then the corresponding output $f(1) - f(n)$ is obtained. After that, a_0 is replaced by the gray value of the second pixel, and the process repeats until all pixels of the secret image are processed. However, in our proposed scheme, the size of each shadow image is $1/r$ of the secret image. The essential idea is to use a polynomial function of order $(r - 1)$ to construct n image shares from a DCT-based transformation matrix with $l \times l$ pixels of the secret image being transformed; $S\_dct(i, j)$ denotes the coefficient value at the (i, j) position after the original secret image is transformed by DCT function. $f_{x\_dct}(i, j)$ denotes the coefficient value of shadow image shares. This method reduces the size of image shares to become $1/r$ of the size of the secret image. Note that any r image shares can be used to reconstruct every pixel value in the secret image. As shown in Fig. 4, the image is separated into multiple shares, which are uploaded to different media clouds. Thus, any one of the clouds cannot disclose the whole information. The user only downloads a certain number of shares from multiple clouds and can recover all of the information.

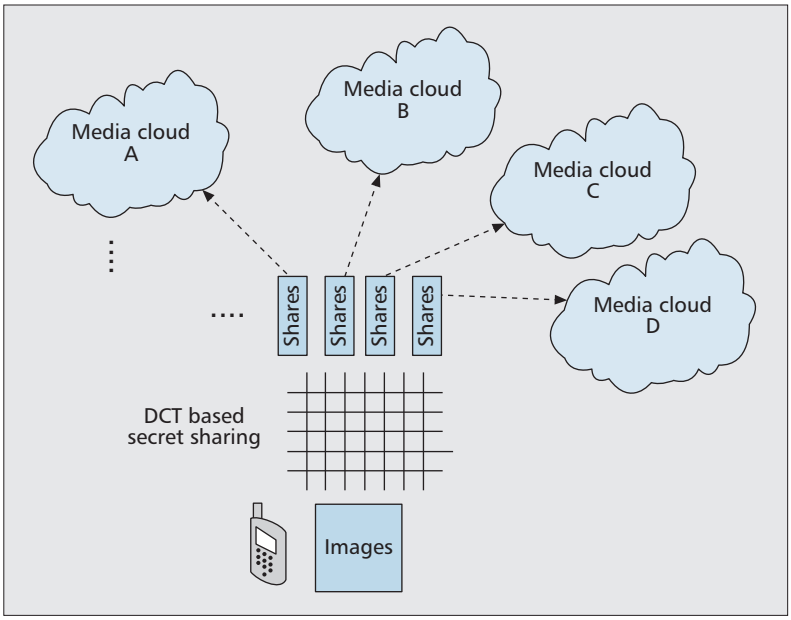

Figure 4. *Secret sharing for the cloud.*

As shown in Table 1, we evaluated our approach on different types of images. We define the noise density at different levels, which indicates the percentage of noise that has been added into the images. We tested our watermarking solutions and compare the peak signal-to-noise ratio (PSNR) of the extracted watermark and its normalized correlation. Our studies show that with the increased noise level, the PSNR of the extracted watermark is gradually decreased. However, with RS code, the extracted watermark quality and correlation are tolerable. Figure 5 represents the normalized correlation (NC) values of the watermark. In our studies, the NC values are obtained when LH3 is an input to RS code. From our studies, it can be concluded that the computation time when LH3 band as input to RS code is less compared to the computation time when the full image is given as input to RS code. By using LH3 band in the extraction process, the scheme reduces computation time and also decreases transmission overheads. We compare the approaches with and without RS. The results indicate that with RS code, the extracted watermark has better correlation with the original watermark. We conclude that the joint

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

Table 1. *With noise and Reed-Solomon code.*

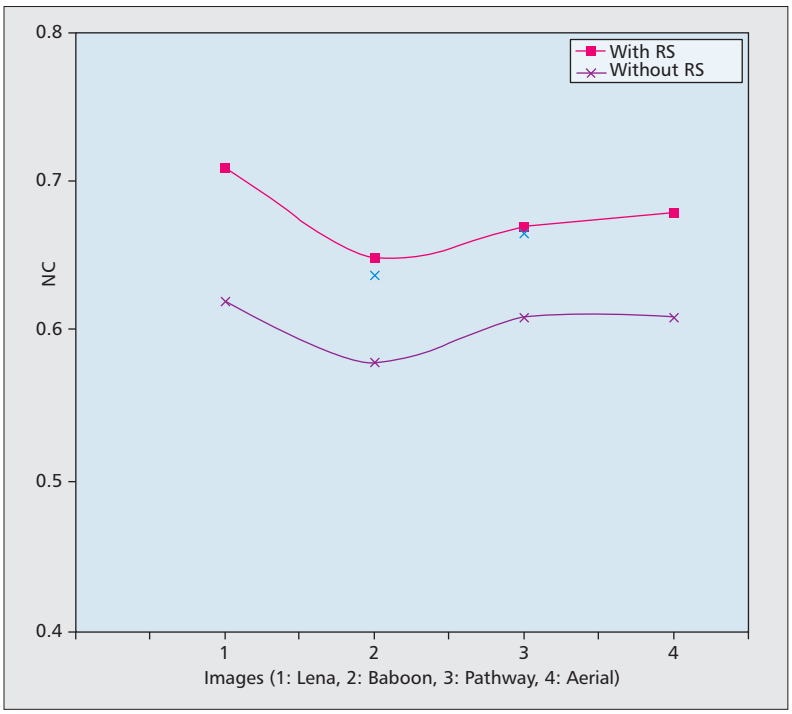

Figure 5. *Normalized correlation.*

design of watermark and RS code can achieve better authentication performance. Due to page limits, we only show some of the studies on our tests of both watermarking and secret sharing schemes.

Conclusion

Security protection between users and the mobile media cloud is critical for future multimedia applications. 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 transmission 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. Our studies show that the proposed approach can effectively improve the security performance level between users and the media cloud. Our research opens a new vista in user-oriented security research for the media cloud.

References

[1] S. Dey, "Cloud Mobile Media: Opportunities, Challenges, and Directions," *Proc. Int'l. Conf. Computing, Networking and Commun.*, 2012, pp. 929–33.

[2] F. Sardis *et al.*, "On the Investigation of Cloud-Based Mobile Media Environments with Service-Populating and QoS-Aware Mechanisms," *IEEE Trans. Multimedia*, vol. 15, no. 4, June 2013, pp. 769–77.

[3] Y. Xu and S. Mao, "A Survey of Mobile Cloud Computing for Rich Media Applications," *IEEE Wireless Commun.*, vol. 20, no. 3, June 2013.

[4] S. Wang and S. Dey, "Adaptive Mobile Cloud Computing to Enable Rich Mobile Multimedia Applications," *IEEE Trans. Multimedia*, vol. 15, no. 4, June 2013, pp. 870–83.

[5] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A Digital Watermark," *Proc. IEEE Int'l. Conf. Image Processing*, vol. 2, 1994, pp. 86–90.

[6] C. F. Wu and W. S. Hsieh, "Image Refining Technique Using Digital Watermarking," *IEEE Trans. Consumer Electronics*, vol. 46, no. 1, Feb. 2000, pp. 1–5.

[7] O. H. Kwon, Y. S. Kim, and R. H. Park, "A Variable Block-Size Dotbased Watermarking method," *IEEE Trans. Consumer Electronics*, vol. 45, no. 4, Nov. 1999, pp. 1221–29.

[8] G. C. Langelaar and R. L. Lagendijk, "Optimal Differential Energy Watermarking of DCT Encoded Images and Video," *IEEE Trans. Image Processing*, vol. 10, no. 1, Jan. 2001, pp. 148–58.

[9] J. Huang and C. Yang, "Image Digital Watermarking Algorithm Using Multi-Resolution Wavelet Ttansform," *Proc. IEEE Int'l. Conf. Systems, Man and Cybernetics*, 2004, pp. 2977–82.

[10] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hiding Digital Watermarks using Multiresolution Wavelet Transform," *IEEE Trans. Industrial Electronics*, vol. 48, no. 5, Oct. 2001, pp. 875–82.

[11] A.J. Choudhury *et al.*, "A Strong User Authentication Framework for Cloud Computing," *Proc. IEEE Asia-Pacific Services Computing Conf.*, 2011, 12–15 Dec. 2011, pp. 110–15.

[12] R. Chow *et al.*, "Authentication in the Clouds: A Framework and Its Application to Mobile Users," *Proc. ACM Cloud Computing Security Wksp.*, 2010, Chicago, IL.

[13] K. Lu, Y. Qian, and H.-H. Chen, "A Secure and Service-Oriented Network Control Framework for WiMAX Networks," *IEEE Commun.Mag.*, vol. 45, no. 5, May 2007, pp. 124–30.

[14] B. Rong *et al.*, "A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study," *IEEE Trans. Vehic. Tech.*, vol. 58, no. 1, Jan. 2009, pp. 398–408.

[15] H.-T. Yeh, B.-C. Chen, and Y.-C. Wu, "Mobile User Authentication System in Cloud Environment," *Security Comm. Networks*.

Biographies

Honggang Wang [SM] (hwang1@umassd.edu) received his Ph.D. degree in computer eEngineering from the University of Nebraska-Lincoln in 2009. He is currently an assistant professor in the Department of Electrical and Computer Engineering at the University of Massachusetts Dartmouth.

His research interests include wireless e-Health, sensor networks, multimedia communications, wireless network, and social networks. He has published more than 100 papers in his research areas. He serves as a chair/co-chair for several international conferences and on the editorial boards of several journals. He was Lead Guest Editor of an *IEEE Journal of Biomedical and Health Informatics* Special Issue on Emerging Wireless Body Area Networks (WBANs) for Ubiquitous Healthcare in 2013.

SHAOEN WU [M] (swu@bsu.edu) received a Ph.D. in computer science in 2008 from Auburn University. He is presently an assistant professor with the Department of Computer Science at Ball State University. He has been an assistant professor in the School of Computing at the University of Southern Mississippi, a researcher scientist at ADTRAN Inc., and a senior software engineer at Bell Laboratories. His current research is in the areas of cyber security, wireless networking, cloud computing, and mobile computing. He was a recipient of Best Paper Awards of IEEE ISCC 2008 and SCS ANSS 2012. He has served as the chair and on committees of several conferences, and as an editor for several journals. His research has been funded by NSF and NASA.

MIN CHEN [SM] (minchen@ieee.org) is a professor in the School of Computer Science and Technology at Huazhong University of Science and Technology. He was an assistant professor in the School of Computer Science and Engineering at Seoul National University (SNU) from September 2009 to February 2012. He worked as a post-doctoral fellow in the Department of Electrical and Computer Engineering of the University of British Columbia for three years. Before joining UBC, he was a post-doctoral fellow at SNU for one and a half years. He has more than 170 paper publications. He received a Best Paper Award from IEEE ICC 2012 and a Best Paper Runner-up Award from QShine 2008. He hasa been a Guest Editor for *IEEE Network*, *IEEE Wireless Communications*, and other publications. He was Symposium Co-Chair for IEEE ICC 2012 and IEEE ICC 2013. He is General Co-Chair for IEEE CIT 2012. He is a TPC member for IEEE INFOCOM 2014. He was Keynote Speaker for CyberC 2012 and Mobiquitous 2012.

WEI WANG [M] (wei.wang@sdstate.edu) is an assistant professor with the Department of Electrical Engineering and Computer Science, South Dakota State University, Brookings. He received his B.S. degree in computer and information engineering from Xian Jiaotong University, China, in 2002, and his M.S. degree in information and communication systems from Xian Jiaotong University, China, in 2005. He received his Ph.D. degree in computer engineering from University of Nebraska-Lincoln in 2009. His major research interests include wireless sensor networks, multimedia computing, information security, and educational robotics. He won two Best Paper Awards at IEEE WCNC 2008 and ANSS 2011. He serves as an Associate Editor of *Wiley Security in Communication Networks Journal*, and as a Guest Editor of three Special Issues for *Hindawi IJDSN* on Energy-Efficient Sensor Networks, Underwater Wireless Sensor Networks, and Data Dissemination in Vehicular Environments. He is Program Chair of ACM RACS 2014, and was Workshop Co-Chair of ICST BodyNets 2013, Chair of the IEEE CIT-MMC track 2012, Vice-Chair of the IEEE ICCT-NGN track 2011, Program Chair of ICST IWMMN 2010, and a Technical Program Committee (TPC) member for many international conferences such as IEEE GLOBECOM, ICC, and WCNC.