# An Efficient Approach for Data Security in Cloud Environment using Watermarking Technique and RSA Digital Signatures

**Uma B[1], Dr. Sumathi S[2]**

*[1]PG Scholar, Dept. of Electronics and Communication Engineering, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.*
*[2]Professor, Dept. of Electronics and Communication Engineering, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.*

---***---

**Abstract -** *Multimedia is the fast growing technology and almost all the mobile users need multimedia based applications. As mobile device have limited storage and simultaneously it cannot process other multimedia (video) application due to small RAM. Therefore we are using cloud for storing our information. But we cannot assure the security of our stored information in the cloud. The maintenance team of cloud environment may provide copyright protection but there is a chance of stealing/hacking our own confidential information by them. Robust reversible watermarking and RSA digital signature can solve this problem. These two techniques were used after the encryption algorithm and is used to protect the data in mobile cloud environment. It offers better security performance, increase the original information quality and confidentiality.*

***Key Words:*** RSA signature, Robust reversible watermarking, data integrity and confidentiality.

## 1.INTRODUCTION

### 1.1 Mobile cloud environment

“Mobile Cloud Computing is an infrastructure in which both the data storage and the data processing happen outside of the mobile device. The basic idea of Mobile Cloud Environment is Cloud Computing. Mobile Cloud Environment is the combination of Mobile Computing, Mobile Internet and Cloud Computing. By using this technology, resources can be shared and stored.

The rapid development of multimedia applications such as electronic publishing, digitized images and videos etc., leads to the requirement of more storage in mobile phones. In order to avoid this problem, we use cloud for storing our information. Data (wireless multimedia applications) access over wireless networks are much faster. But we are not assured of data security. So the RSA digital signature and Robust Reversible Watermarking is used to solve the above mentioned problem.

Data security in mobile cloud environment has to ensure the secured and reliable multimedia data transmissions between mobile users and the mobile cloud. However, the mobile cloud is maintained by third parties such as mobile cloud service providers and we cannot be trust them at all time. We can have contracts between users and mobile cloud service providers in order to ensure data security. This arise some potential risks, such as security attacks or misconduct of the mobile cloud provider. But users can trust themselves rather than mobile cloud security providers. Our design is user-oriented, and allows users to protect their data’s security and privacy.

The receiver should have the confidence that the public key belongs to the originator otherwise any substitution by a duplicate public key would enable a "man in the middle attack" to negotiate the data. One mechanism for stating the authority of the relationship among the originator and their public key depend on certificates. They are issued by trusted authorities who generate and digitally sign certificates requisite entities (such as people and organisations) to their public keys. Unfortunately, mechanisms enable us to trust the signature of the trusted authority on the certificate.

### 1.2 RSA algorithm

RSA algorithm can be used to encrypt and decrypt the data being signed. RSA does not demand a particular hash function. So the protection of the signature and encryption are partly dependent on the choice of hash function used to compute the signature. It is an asymmetric cryptographic algorithm. RSA algorithm involves two keys: public key and private key. The public key is known to everyone, it is used to encrypt messages. Messages encrypted with a public key can be decrypted only with a private key. RSA algorithm can be used for key exchange, digital signatures, or encryption of small block data. This algorithm uses variable size encryption block and variable size key. RSA algorithm is widely used for establishing secure communications, authentication and the identity of service provider over insecure communication. In proposed scheme, RSA algorithm is used to find out the key pair for both mobile user and cloud service provider. These keys are used to encrypt and decrypt the file. These two operations: *sign* and *verify*.

If the signature generated is different or after being signed if the message is altered, then the chances of the verifying correctness are extremely small. The first step in generating an RSA signature is to apply a cryptographic hash function (reduces the message length to a short number, called the "hash value-160 bits long") with two conditions being satisfied:

- It is HARD to find a message with a specific or particular hash value.
- It is HARD to find two messages having same hash value.

Then the hash value is converted into an integer called the "message representative," with a length that is the same as the length of the RSA key. This is completed by applying a padding format to the resultant hash value or embedding the hash value to generate the message representative. In addition to this, padding format also provides additional security and serves as the primary differentiator among the several RSA signature schemes. The final step applies the RSA original signature to the message representative with the help of RSA private key to generate the signature.

To forge a signature, an attacker needs to compute the RSA signature primitive without knowing the private key. The signature verification process is

$$S^e=Pad(Hash(M))(mod\ N)$$

Where S is the signature; M is the message; e and N are the public exponent and modulus from the public key; (mod N) means that equality is checked modulo N; Pad is the padding function; and Hash is the hashing function.

### 1.3 HASH function

A cryptographic hash function uses a message of arbitrary length and creates a message with fixed length. A hash function produces short and fixed length message, which is unique for each message. The main and foremost condition for the security of hash functions is that they should be one-way functions. Here in the proposed scheme hash of file is calculated so that integrity can be maintained.

- **Data Owner:** Person who owns the data which is to be stored in cloud.
- **Third Party Auditor:** Mediator between the Data Owner and Cloud Service Provider checks the integrity of the data stored on mobile cloud.
- **Cloud Service Provider:** Cloud Service Provider provides the storage services to the mobile users.

Third party Auditor checks the hash value and message to verify the integrity of the data. The integrity certification is given by the third party auditor which reduces a lot of work of the mobile user. In proposed method, RSA algorithm is used for performing encryption and decryption which affords message authentication. The hash function of the message is also calculated to provide security to the data.

### 1.4 Reversible watermarking technique

The art of secretly smacking and communicating information has increased the importance in the last two decades due to the progresses in generation, storage, and communication technology of digital content. Therefore, at the receiving end, the exact recovery of cover work may not be possible. Additionally, there occur certain applications that may not withstand even small alterations in cover work preceding to the downstream processing. In such kind of applications, reversible watermarking instead of conventional watermarking is employed. Reversible watermarking of digital content permits full extraction of the watermark along with the complete restoration of the cover work. There is a rapid evolution of reversible watermarking techniques and is highly desirable.

## 2. EXISTING WORK AND METHODOLOGY

In existing methods, traditional watermarking is used for data security while interacting among the mobile users and mobile cloud. Watermarking is one of the promising solutions for damage detection and protection of digital content. However, watermarking can cause damage to the delicate data present in the original information. Due to this, original information is easily corrupted. Therefore restoration of original data from the mobile cloud becomes a major issue making traditional encryption algorithms are less effective.

In existing method, old compression algorithms are used before encryption and watermarking. The approach used in this paper hides target image in the host image using image watermarking and then it applies RSA algorithm for protecting watermarked image from tempering and subsequently it uses dictionary based compression approach to reduce size of encrypted watermarked image. The disadvantages of existing method are as follows: less effective, losses in recovery of original image, attacks from unauthorized users.

### 2.1 Methodology

The Asymmetric Encryption and robust reversible Watermarking Technique is used for securing the data in the mobile cloud environment which is less secure compared with our proposed work. An improved PSNR value is achieved in our proposed method.

## 2.2 Proposed work

Fig-1 shows the proposed work. In this paper, data security is enhanced using a combination of RSA digital signature algorithm with robust reversible watermarking technique. Reversible watermarking allows full extraction of the watermarked image along with the complete restoration of the original data from the mobile cloud.

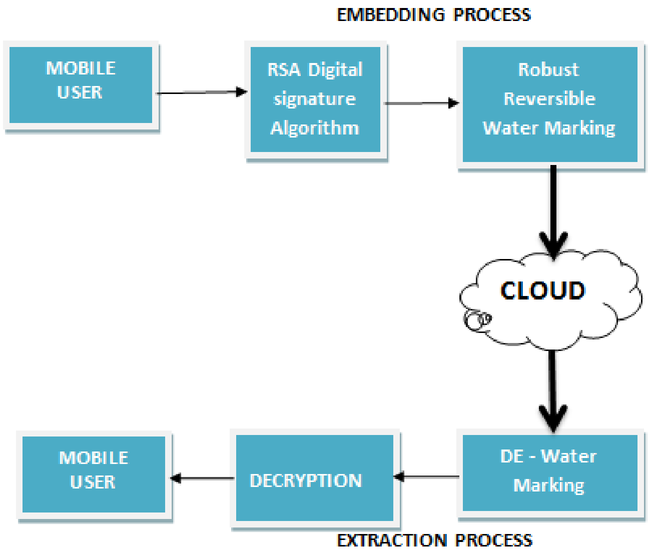


**Fig -1**. Proposed Work

## 2.3 Encryption and watermarking process

, A confidential message is created by the mobile user to the mobile cloud via internet. That message is encrypted using RSA digital signatures (generates a public and private key) and the information is then watermarked using robust reversible watermarking algorithm in the cover image. Then the created embedded image is sent through internet and stored in the mobile cloud environment.

## 2.4 Decryption and de-watermarking process

STEP-1:Embedded image is extracted using reversible algorithm.

STEP-2:Extraction of the secret message and cover image is separated.

STEP-3:Decrypt the message with the generated hash value and compare it with the hash value generated in encryption side.

STEP-4:If hash values are same, then the message will be decrypted or else it will not be decrypted.

## 3. RSA DIGITAL SIGNATURE

Digital signatures are increasing their importance as they gain authorized standing with traditional handwritten signatures. The RSA digital signature scheme applies the sender's private key to a message to generate a signature. The signature can then be verified by applying the corresponding public key to the message and the signature in the verification process, generating either a valid or invalid result. These two operations: sign and verify, comprise the RSA digital signature scheme. In fig-2 paradigm refers to input.

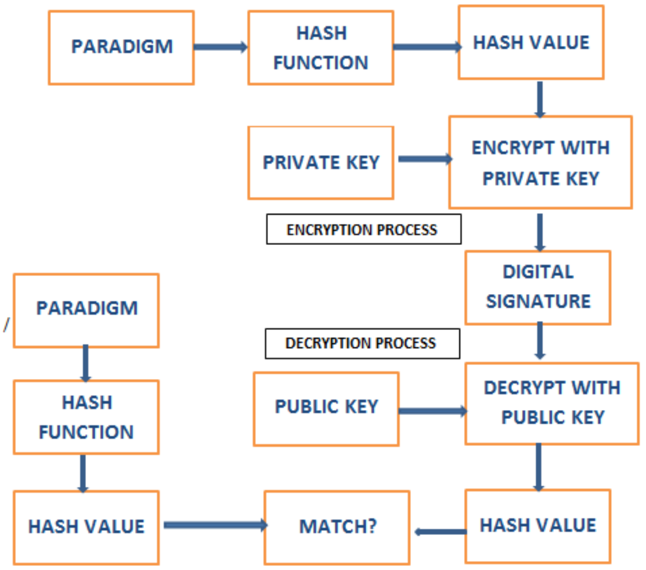


**Fig-2** Creation and Verification steps of Digital Signature

Fig-2 shows how the hash value is encrypted using either a public or private key.

## 4. ROBUST REVERSIBLE WATERMARKING

The promising solutions for watermarking are one of digital content for tamper detection and protection. However, watermarking can cause damage to the sensitive information present in the work under cover. At the receiving end, the recovery of cover work extract may not be possible. Additionally, there exist certain applications that may not tolerate even small distortions in work cover prior to the downstream processing. In process applications, reversible watermarking instead of conventional watermarking is employed. Reversible watermarking allows full extraction of the watermark along with the complete restoration of the work. For the last few years, reversible watermarking techniques are gaining popularity because of increasing some applications in sensitive and important areas, i.e., important military communication, medical department, and some law-enforcement. Due to the fast evolution of reversible watermarking techniques, a most recent review of research in this area is highly desirable.

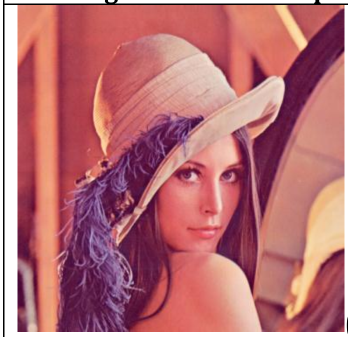
## 5. SOFTWARE TOOL

MATLAB R2009b/MATLAB R2012a software is used.

## 6. RESULTS AND DISCUSSIONS

In this section, we demonstrate the effectiveness of our proposed methodology. The simulation is done on MATLAB2012a & analysis of PSNR and robustness of image. This method is applied to several images having different types of pixels. The first figure in Table-1 is a 512X512 image which is encrypted and embedded using 128 bytes of plain text and 128 bytes of original image in our experiment. In [1], the PSNR value for the same image is 34.1 dB. In our proposed method, the achieved PSNR value 43.626 dB. At the receiver side, data is extracted not with data loss. Other than this, PSNR values are calculated using different images having various pixel size and is listed below.

**Table-1** Images with different PSNR values

| Image with different pixel size. | PSNR (dB) |
|---|---|
| (512×512) | 43.626 |
| (300×168) | 44.597 |
| (300×168) | 44.3614 |

### 6.1 Discussion

#### 6.1.1 PSNR

It is the ratio between the maximum probable power of a signal and the power of corrupting noise that influences the fidelity of its representation. For this reason that many signals have a extremely extensive dynamic range. PSNR is typically expressed in terms of the logarithmic decibel scale. The PSNR (in dB) is defined as

$$MSE = \sum_{M,N}[I(m,n) - J(m,n)]^2/(M * N)$$

Where,

$M$ and $N$ are the number of rows and columns in the input images

$$PSNR = 10\log_{10}(R^2/MSE)\ dB$$

Where,

$R$ is the maximum fluctuation in the input image data type and typically its equal to 255.

## 7. CONCLUSION AND FUTURE ENHANCEMENTS

In this paper, the proposed method has enhanced the data security between mobile user and mobile cloud environment. The combination of RSA digital signature and Robust Reversible watermarking is used to improve the data confidentiality and security for sending information to the mobile cloud providers. Along with this, generation of an image key from the encrypted watermarked image increases the security. Surely the complexity of the process increases but at the same time an improved security is achieved. Future scope is to test implement the same algorithm on video and other multimedia contents. We also change the combination of encryption algorithms with different watermarking algorithms to improve the output message without any loss.

## REFERENCES

[1] Deepika Verma, Er. Karan Mahajan,(December 2014), 'To Enhance Data Security in Cloud Computing using Combination of Encryption Algorithms', International Journal of Advances in Science and Technology (IJAST) ,Vol 2, Issue 4.

[2] Ankita Ojha, Tripti Sarema, Dr.Vineet Richariya, (May 2015),'An efficient approach of sensitivearea watermarking with encryptionsecurity', International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 4 Issue 5.

[3] Honggang Wang,Shaoen Wu, Min Chen Wei Wang, (March 2014)'Security protection between users and the mobile media cloud',IEEE communications magazine.

[4] Jagruti R. Mahajan, Nitin N. Patil, (2015) 'Alpha channel for integrity verification using digital signature on reversible watermarking QR', international conference on computing communication control and automation.

[5] A.Khan, A.Siddiqa, S.Munib, and S.A.Malik, (2014), 'A Recent Survey of Reversible Watermarking Techniques', DOI:10.1016/j.ins.2014.03.118, Information Sciences.

[6] Dharini. A, R.M. Saranya Devi, and I. Chandrasekhar, (Nov. 2014), 'Data Security for Cloud Computing Using RSA with Magic Square Algorithm', International Journal of Innovation and Scientific Research,ISSN 2351-8014 Vol. 11 No. 2 pp. 439-444, 2014 Innovative Space of Scientific Research Journals.

[7] Manish gupta, Darpan Anand, Rajeev gupta, Girish parmar,(November 2012), 'A new approach for information security using asymmetric encryption and watermarking technique', international journal of computer applications (0975 – 8887), volume 57– no.14.

[8] Mamatha, Pradeep Kanchan, (June 2015), 'Use of Digital Signature with Diffie Hellman KeyExchange and Hybrid Cryptographic algorithm toEnhance Data Security in Cloud Computing', International Journal of Scientific and Research Publications, Volume 5, Issue 6, 1 ISSN 2250-3153.

[9] Mayank Patwal, Tanushri Mittal, (March 2014), 'A Survey ofCryptographic basedSecurity Algorithms forCloud Computing', HCTL Open Int. J. of Technology Innovations and Research HCTL Open IJTIR, Volume 8, e-ISSN: 2321-1814 ISBN (Print): 978-1-62951-499-4.

[10] Navnath Narawade, Rajendra Kanphade, (June 2011), 'Reversible Watermarking: A Complete Review', International Journal of Computer Science and Telecommunications, Volume 2, Issue 3.

[11] Pradeep Bhosale, Priyanka Deshmukh, Girish Dimbar, Ashwini Deshpande, (October - 2012), 'Enhancing Data Security in Cloud Computing Using 3D Framework &Digital Signature with Encryption', International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8.

[12] Prayas Gajbhiye, Arati Dandavate, (April 2016), 'Secure Sharing and Searching forReal-Time Video Data in Mobile Cloud: ASurvey',International Journal of Innovative Research in Computerand Communication Engineering(An ISO 3297: 2007 Certified Organization)Vol. 4, Issue 4.

[13] Rachna Arora, Anshu Parashar, (Jul-Aug 2013), Secure User Data in Cloud Computing Using EncryptionAlgorithmsInternational Journal of Engineering Research andApplications (IJERA) ISSN: 2248-9622Vol. 3, Issue 4, , pp.1922-19261922

[14] Randeep Kaur, Supriya Kinger, (March 2014), 'Analysis of Security Algorithms in CloudComputing',International Journal of Application or Innovation in Engineering & Management (IJAIEM)Web Site: www.ijaiem.org Email: editor@ijaiem.orgVolume 3, Issue 3.

[15] Reenu Lathwal, Vinod Kumar Saroha,(Jan 2016), 'A Survey on Data Encryption in CloudUsing KDC', International Journal of Computer Science Engineering (IJCSE), ISSN 2319-7323 Vol. 5 No.01.

[16] Shakun Gupta, Harsimran Singh, (2015) 'To Propose A Novel Technique for Watermarking in Cloud Computing', International Journal of Engineering Development and Research, IJEDR Volume 3, Issue 2 | ISSN: 2321-9939.

[17] Shreya Srivastava, Neeraj Verma, (July 2015), 'Improving Data Security in Cloud Computing Using RSA Algorithm and MD5 Algorithm', International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization), Vol. 4, Issue 7.

[18] Sidham Abhilash, S M Shamseerdaula, (Nov-Dec 2013), 'A Novel Lossless Robust Reversible Watermarking Method forCopyright Protection of Images',Journal of Engineering Research and Applications www.ijera.com, ISSN : 2248-9622, Vol. 3, Issue 6, pp.317-323

[19] Suresh p, Varun Kumar M N, (2013) 'An efficient model and security framework for data storage in mobile cloud computing using RSA algorithm and hash function', international journal of research in science & engineering e-ISSN: 2394-8299 volume: 1 special issue: 2 p-ISSN: 2394-8280.

[20] M.Srivenkatesh, K.Vanitha, (April 2015), 'Implementing Multiprime RSA Algorithm to Enhance the Data Security in Federated Cloud Computing',International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 4Copyright to IJARCCE DOI 10.17148/IJARCCE.2015.44149 647.