Enhanced Data Security using RSA Digital Signature with Robust Reversible Watermarking Algorithm in Cloud Environment

[1]Monisha.M.S, [2]Chidambaram.S
[1,2]Dept. of ECE, Adhiyamaan College of Engineering, Hosur, TN, India

Abstract

Nowadays multimedia is a fast growing technology and almost all the mobile users would need for multimedia based applications in mobile phones. In multimedia cloud due to its increasing demand, and millions of users can surfing for various purpose, therefore threat of its security is becoming a major issue. Several old security methods are suggested to secure the interaction between the mobile user and cloud environment. In traditional watermarking can cause damage to the sensitive information present in the original data. We know that the most secure web transactions today are already dependent on RSA algorithm.In our research work RSA digital signature algorithm used for encryptionprocess. After the encryption algorithm,the scalable watermarking method is used to ensure the data integrity and confidentiality, which is a robust reversible watermarking used to watermark the encrypted sending message to enhance the data security and prevent access from the unauthorized users. In our work both RSA digital signature and robust reversible watermarking is used to protect the data in mobile application environment efficiently. Our research findings shows that the proposed method not only reaches better security performance, but also recover the original information and enhance the confidentiality purpose.

Keywords

Cloud Environment, Data Security, Traditional Watermarking, RSA Digital Signature, Robust Reversible Watermarking.

I. Introduction

Due to development of information technology in recent years, electronic distributing such as sharing of digitized images and Information, is becoming widespread. Through the internet with mobile phone the multimedia content can easily sent all over the world using cloud system.As a result of fast growing multimedia applications the security has become a progressively more concern for media access control[1]. For this reason, we need to ensure secure and consistent multimedia data transmission between mobile users and Cloud environment.

In order to attain the secure transmission and retain the integrity of transferring data using special concern to protect these contents from unauthorised users[2]. Cloud environment, cloud users may inquest the data from sensing devices. A stored sensitive data is processed outside the mobile devices on a centralized platform located in clouds [3]. The data sent by mobile users is very sensitive, so that any hackers can do changes on it, to maltreatment the data. Specifically, the cloud providers are responsible for media cloud servers therefore users not fully trusted while storing the file in the cloud server [4].Cloud computing provide the required services to the users on paid basis[5].Theusers can access the cloud services without any previous knowledge on managing the resources.User access their databases anywhere in the world only when connected to the internet. Currently, users can store their private and public data on media cloud computing. As a result, security in cloud computing has required lots of consideration. Combination of RSA encryption algorithm and digital signature technique provides several way of security that is data security, confidentiality and integrity [10].At present most of the business depends on communication for transferring their high security databases[13]. Rapid development of internet usage all over world, attacks also increase enormously. Therefore the traditional encryption not sufficient for security over internet.

However the security for transmitting and receiving the data to user from the media cloud application is improved in our proposed work using both encryption algorithm and robust reversible watermarking algorithm, and also computedMSE and PSNR for information.

II. RSA Digital Signature Algorithm

Today tremendous opportunities are present in electronic transactions of all categories through internet, suggestively need for the paper documentations are reduced. As a result trust established for digital signature are supposed to enter in electronic transactions as a primary vehicle.

RSA digital signature is one of most secure web transaction today, most of the transactions are depend on these algorithms. In transaction, as a part of the digital certificate a server presents to a client to identify itself. It is one of most popular and demonstrated asymmetric key cryptographic algorithm[7]. It consist of two keys public and private. Three types of services provided by the digital signature that is authentication, data integrity and non-refutation, but using these digital signature the confidentiality is difficult one because of transferring data is very sensitive [12]. Using the concept of public key encryption we can achieve this confidentiality in transferring the data[11].

RSA algorithm involves three steps:

- Key Generation
- Encryption
- Decryption

The digital certificate binds a public key that is an identity for sender and the receiver to verify their secure connection with a web server.

The user have own authorisation to get the original information from the server and also only authorised user can decrypt it [8]. In RSA digital signature scheme using the sender's private key applied to message and generate a signature, the signature can then be verified by applying the corresponding public key to the message and the signature through the verification process, providing either a valid or invalid result.

A. Hash Function

To reduce a message of any length to a short number, called the "hash value". Generating a digital signature is applying a cryptographic hash function to the message. Sending information is selected, corresponding hash value is find.

III. Robust Reversible Watermarking

Protection of multimedia content becoming major issue because of consumer insufficient perception of the rights to intelligent property.Currently, researchers all over the world are highly focusing, for protecting the ownership of the digital content.

Digital watermarking is a process of embedding digital information called watermark into a multimedia. One of the important application for digital watermarking is copyright protection. Robustness is one of the most commonly measured properties is that watermark signals must be reasonably resilient to various stacks and common signal processing operations in digital watermarking systems [6].

For the digital watermarking of images, the good watermarking method is likely to resist against noise addition, filtering process, geometrical transformations such as scaling, translation, and rotation. Complete renovation of the cover work along with the extraction of watermark is fully recovered in digital content using reversible watermarking. Due to its growing applications in some important and delicate areas reversible watermarking techniques are become highly desirable [9].

IV. Proposed system

In proposed method to enhance the data security we are using the combination of RSA digital signatures algorithm with robust reversible watermarking. Reversible watermarking of digital content allows full extraction of the watermark along with the complete renovation of the original data from the cloud. For improving the security to restrict the extracting and un-authorized deletion from an image. Transmitted side block diagram is shown in fig. 1.

A. Transmitting Side

In Embedding process the mobile user send the secret message to the cloud through internet. The sending message is encrypted with the help of RSA digital signatures and the information is watermarked in the cover image with the help of robust reversible watermarking algorithm then the embedded watermarked image is created and finally add the noise to the embedded image that is stored in the mobile application environment.

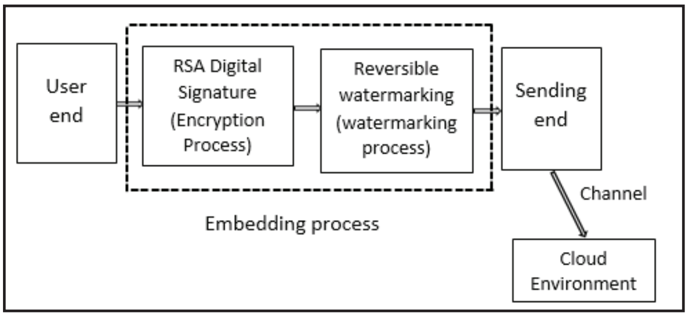

User end
RSA Digital Signature (Encryption Process)
Reversible watermarking (watermarking process)
Sending end
Channel
Embedding process
Cloud Environment

Fig. 1: Transmitting Side

Embedding Process: First our secret information is selected and corresponding hash value is computed. Hash value is encrypted with the private key of the sender.The key generation is based on RSA algorithm. Encrypted hash is watermarked using reversible watermarking into cover image and also noise could be added to the cover image. Finally embedded image is created is shown in fig. 2.

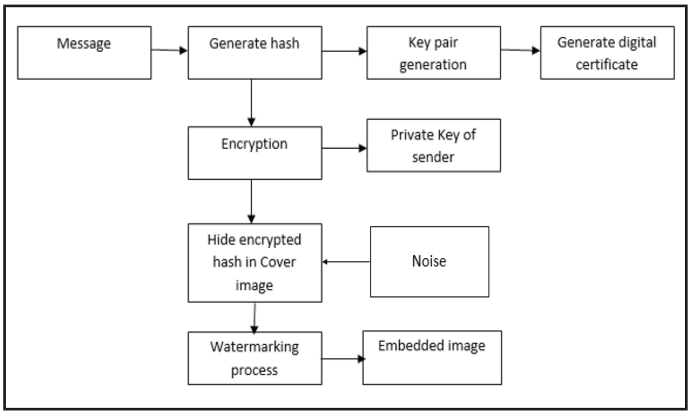


Fig. 2: Embedding Process

B. Receiving Side

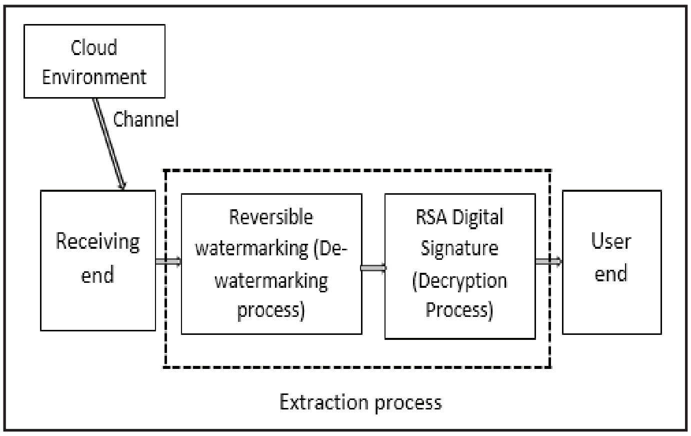

Cloud Environment
Channel
Receiving end
Reversible watermarking (De-watermarking process)
RSA Digital Signature (Decryption Process)
User end
Extraction process

Fig. 3: Receiving Side

Block diagram of the receiving process is shown in fig. 3. In receiving side extracting the original image for that, user send the request to cloud, therefore user send the (signature) for authentication purpose to get original encryption image. Cloud itself compare the (signature) and send the embedded image to the user. The embedded image is then de-watermarked. The result of de-watermarking separate the cover image, noise and encrypted message.

Then the encrypted message is decrypted we get the hash value and finally the compare the result has value to our own hash value, it is valid means the authorized user get the original sending message from mobile application cloud.

Extracting Process: The stored image is extracted from the cloud service provider. From the embedded image the cover image with noise and encrypted hash value is separated. Finally de-noised cover image is separated from the cover image and after decryption the hash value is compare with our own hash value. After comparison the result is valid then only we receive our original message that is given in fig. 4.

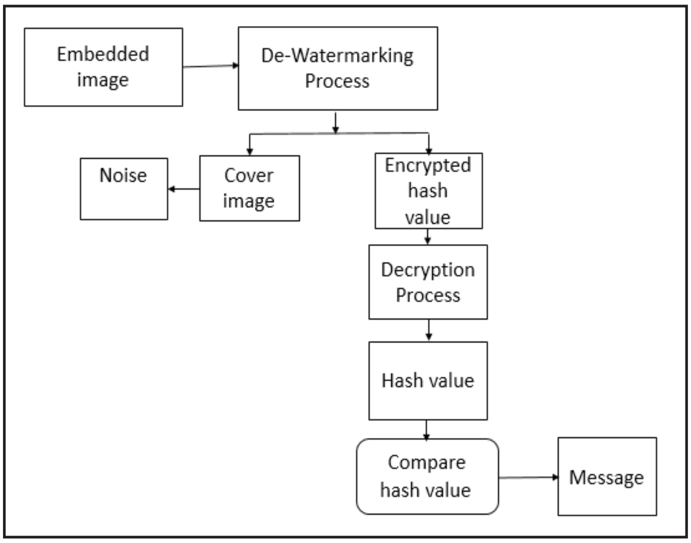


Fig. 4: Extracting Process

C. Algorithm Description

(i). Encryption and decryption with key pair generation-RSA

Step 1: select p, q p and q both prime, p ≠ q
Step 2: Calculate n= p × q
Step 3: Calculate Φ (n) = (p-1) (q-1)
Step 4: Select integer e
Step 5: calculate d d= e^{-1}(mod (Φ (n))
Step 6: Private key PR = {d, n}
Step 7: Decryption M= C^d mod n

(ii). Reversible watermarking using LSB Substitution for watermarking process

Step 1: Take two adjacent pixel values of x and y
Step 2: Find difference and average values of pixels
Step 3: Then we expand into its binary form and add watermark bit right after most significant bit to get
Step 4: Reconstruct the image using and d', we get the watermarked image

V. Results and Discussion

In our research, with the use of two algorithms the security of the sending data is enhanced and the results are given below,

A. Empirical Work

1. Transmitting side

Input Message: Adhiyamaan College of Engineering

Hash Value: From the above message corresponding hash value is created.

Embedded Image: Subsequently the encryption hash value is created. Simultaneously the cover image is added with noise and Noisy cover image is created. The encrypted hash value is embedding into noisy cover image, finally at the transmitting side embedded image (watermarked image) is created.

Watermarked Image: This image is sending through channel and stored in cloud environment.

2. Receiving Side

Recover the original message from the cloud environment.

Extracting process: Separate the encrypted hash1 value, De-watermarked noisy cover image, finally cover image is extracted without loss. Encrypted hash value is decrypted and the corresponding hash value is compared with our own hash value.After comparison the valid message is received from the cloud environment.

Decryption Process: User send the private key to get the secret message from the cloud, and that key also usedto compare the hash value to our own hash value the authorised user can get the secret message. The recovery original image quality is characterised using two parameters that is MSE and PSNR.

Mean Square Error:

$$MSE = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I(x,y) - I'(x,y)\right)^2$$

Peak Signal-to-Noise Ratio:

$$PSNR = 10\lg\left[\frac{M \times N \times 255^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I(x,y) - I'(x,y)\right)}\right]$$

3. Comparative Analysis of Different Images

Table 1 lists the different image and their corresponding MSE and PSNR values for noise range 0.02.

Table 1: Images Analysis With Noise (Salt and Pepper)= 0.02

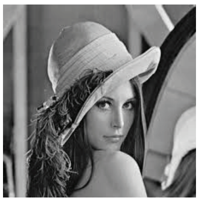
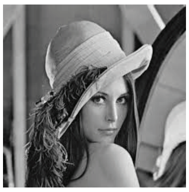
IMAGE	MSE	PSNR (dB)
 Barbara	0.00050	38.630
 Lena	0.00053	38.507
 Beach house	0.00027	39.870
 Peppers	0.00054	38.496

Table 2 lists the different image and their corresponding MSE and PSNR values for noise range 0.05.

Table 2: Images Analysis with Noise (Salt and Pepper) = 0.05

IMAGE	MSE	PSNR (dB)
Barbara	0.00054	38.460
 Lena	0.00051	39.593
Beach house	0.00017	40.741
Peppers	0.00050	38.630

VI. Conclusion

In this paper the proposed method should enhance the data security between user and cloud environment. The combination of RSA digital signature and Robust Reversible watermarking which is used to improve the data confidentiality and security for sending information to the cloud providers. Our major concern is only how to increase the data security for sending and receiving the information in the mobile application cloud environment. Our paper also given the output message is extracted from the cloud environment efficiently without any loss. Using RSA is already accepted as a secure public key encryption algorithm and watermarking is also technique to provide the information security. Along with this we generate an image key from the encrypted watermarked image, it increases the security. Surely the complexity of the process increases but at the same time the improved security is achieved.

References

[1] Honggang Wang, Shaoen Wu , Min Chen, Wei Wang, “Security protection between users and the mobile media cloud,” IEEE communications magazine, Vol. 52, Issue. 3, pp. 73-79, March 2014.

[2] Manish Gupta, Darpan Anand, Rajeev Gupta, Girish Parmar,“A new approach for information security using asymmetric encryption and watermarking technique”, International journal of computer applications, Vol. 57, No. 14, November 2012.

[3] Suresh P, Varun Kumar M N,“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, Vol. 1, Special Issue: 2, pp. 162-166, 2013.

[4] Shakun Gupta, Harsimran Singh,“To Propose A Novel Technique for Watermarking in Cloud Computing,” International Journal of Engineering Development and Research, (IJEDR) Vol. 3, Issue 2, 2015.

[5] A. Dharini, R.M. Saranya Devi, I. Chandrasekhar,“Data Security for Cloud Computing Using RSA with Magic Square Algorithm,” International Journal of Innovation and Scientific Research,Vol. 11, No. 2, pp. 439-444, Nov. 2014.

[6] M. Kim, D. Li, S. Hong,“A Robust Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method,” International Journal of Multimedia and Ubiquitous Engineering, Vol. 9, No. 1, pp. 369-378, 2014.

[7] Shreya Srivastava, Neeraj Verma,“Improving Data Security in Cloud Computing Using RSA Algorithm and MD5 Algorithm,” International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 7, pp. 5450-5457, July 2015.

[8] Deepika Verma, Er. Karan Mahajan,"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, pp. 41-44, December 2014.

[9] Asifullah Khan, Ayesha Siddiqa, Summuyya Munib, Sana Ambreen Malik, “A recent survey of reversible watermarking techniques,” Information Sciences Elsevier publication, pp. 251–272, 2014.

[10] Sudhansu Ranjan Lenka, Biswaranjan Nayak,“Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm,” International Journal of Computer Science Trends and Technology (IJCST) – Vol. 2 Issue 3, pp. 60-64, June-2014.

[11] Swapna V. Tikore, Deshmukh Pradeep K., Dhainje Prakash B,“Ensuring the Data Integrity and Confidentiality in Cloud Storage Using Hash Function and TPA,” International Journal on Recent and Innovation Trends in Computing and Communication Vol. 3, pp. 2736 - 2740 Issue 5, May 2015.

[12] Kamal Kr. Gola, Bhumika Gupta, Zubair Iqbal,“Modified RSA Digital Signature Scheme for Data Confidentiality,” International Journal of Computer Applications,Vol. 106 , No. 13, pp. 13-16 , November 2014

[13] Mamatha, Pradeep Kanchan,“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, Vol.5, Issue 6, June 2015.

[14] Hai Tao, Li Chongmin, Jasni Mohamad Zain, Ahmed N. Abdalla,“Robust Image Watermarking Theories and Techniques: A Review,” Journal of Applied Research and Technology, Vol. 12, pp. 122- 138, Feb 2014.

[15] Ankita Ojha, Tripti Sarema, Dr. Vineet Richariya, (May 2015),“An efficient approach of sensitive area watermarking with encryption security,” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol. 4, Issue 5.

M.S.Monisha is pursuing M.E in Communication Systems in the Department of Electronics and Communication Engineering at Adhiyamaan College of Engineering, India. She received his B.E degree in Electronics and Communication Engineering from Anna University, India in 2015. Her research interests are in the domain of Multimedia communication, Image processing and Networks. She is Associate member of IE (The Institution of Engineers).

S.Chidambaram is working as Associate Professor in the Department of Electronics and Communication Engineering at Adhiyamaan College of Engineering, India, where he leads the Image and Signal Processing Lab. He received his B.E degree in Electronics and Communication Engineering from Bharathidasan University, India in 2002, M.E degree in Power Electronics and Drives from Anna University, India in 2005 and currently he is working toward his Ph.D. in the domain of hyperspectral Image Processing. His research interests lie in the field of Digital Signal Processing, Hyperspectral Image processing and Satellite Image Processing such as enhancement, classification and compression algorithms, Statistical Signal Processing, Sparse Representations. He is a member of IEEE and ISTE.