International Journal of Research in Engineering, Science and Management
Volume-2, Issue-7, July-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Review of Multimedia Cryptography Techniques

Tarun Kumar Mishra[1], Mamta Sakpal[2]
[1]Student, Department of Computer Science and Engineering, Poornima College of Engineering, Jaipur, India
[2]Assistant Professor, Dept. of Computer Science and Engg., Poornima College of Engineering, Jaipur, India

***Abstract*: Multimedia Cryptography is a complex process of hiding textual information into a multimedia file or it can be vice versa as well. A non-multimedia file can also accommodate a multimedia file given that its size or the pixel count is more than that of the container file. Cryptography is an essential part of data security services and data preserving and copyrighting preservence. Cryptography can also be termed as steganography, watermarking and etc.**

***Keywords*: Cryptography, Steganography, Watermarking, Multimedia Files, Text Files.**

1. Introduction

RYPTOGRAPHY is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email. Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing. Digital watermarking is the method of embedding data into digital multimedia content. This is used to verify the credibility of the content or to recognize the identity of the digital content's owner.

Digital watermarking can be employed for multiple purposes, such as:

- Copyright protection
- Source tracking
- Broadcast tracking, such as watermarked videos from global news organizations
- Hidden communication

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type. Data security is also known as information security (IS) or computer security.

2. Literature survey

Development of the internet in recent years has led to tremendous increase in demands for multimedia applications [1]. Most of the devices like mobile phones, cars, electronic appliances depend on internet for sharing the multimedia data with other users [2]. Due to this development, data management has become a tougher job [3]. The major problem with data management is the requirement of memory for storing it. As these smart devices come with limited memory and storage capacity, one of the easiest ways to store and manage data is to make use of the cloud [4]. Cloud enables people to store, transmit and receive data anytime provided they are connected to the internet. As data are not directly managed by the owner, threat to data security and privacy increases [5]. This can be avoided by limiting data access and by hiding the data from cloud services that cannot be trusted [6]. Hiding data from the cloud services involves encrypting the data before storing it into the cloud [7-13]. Data encryption not only helps to hide data but also to share data securely across an open source network or the environment. Cryptography can be used to encrypt the files to be shared with the other users in multimedia applications.

Yinghui Zhang, et al., [1] proposed PASH, a privacy aware smart-health access control system based on CP-ABE scheme that supports large universe and partially hidden access policies to efficiently address both data security and user privacy issues in smart-health. Zhen Wang, et al., [2] proposed an enhanced secure instant messaging system that was based on the elliptic curve cryptosystem which supports offline key agreement between users, utilizes timestamps to deny replaying attacks and ECDSA to sign and verify the messages that are transferred in the system. Abid Mehmood, et al., [3] presented an authentication system based on elliptic curve cryptography that utilizes rotating group signature and onion router to provide complete privacy and anonymity to the users from adversaries and authentication server. Kan Yang, et al., [4] proposed a cryptographic approach for cloud-based video content sharing that embeds both the cipher-texts and session keys in time division way such that only users who hold sufficient attributes in a specific time period can decrypt the data. Jiguo Li, et al., [5] presented an efficient user collision avoidance attribute revocation by bounding together the user's private key and group secret key for the cloud storage system. Kaiping Xue, et al., [6] proposed a new solution that combines the cloud-side access control and the existing data owner-side CP-ABE based access control using protocols, bloom filter and probabilistic check to resolve the security problems in privacy preserving cloud storage. Jianting Ning, et al., [7] proposed an auditable σ-time outsourced CP-ABE scheme based on a key encapsulation mechanism that was able to offload pairing operations to the Cloud and provided more flexible access control. Sheng ding, et al., [8] presented a new way of key distribution that uses linear secret sharing structure to enhance the expressiveness of the access policy and revokes a user or an attribute directly without updating other users' keys during the attribute revocation phase. Qiang Wang, et al., [9] proposed a concrete CP-ABE-ET scheme using bilinear pairing and vijete's formulas to provide users with searching capability on cipher-texts and fine-grained access control. Jianghong Wei, et al., [10] presented a novel multi authority CP-ABE scheme that supports scalable user revocation, public secret key and cipher text update to provide both forward security and backward security. Shuming Qiu, et al., [11] presented an improved mutual authentication scheme based on ECC that consists of registration phase, authentication and key agreement phase, and password changing phase to resist off-line password guessing attack, user and server impersonation attack and man-in middle attack in telecare medical system. Sorina Dumitrescu, et al., [12] proposed a general framework for the detection of the least significant bit steganography using image, video and audio as cover objects by estimation of the length of a secret message hidden in the LSBs of samples in which underlying signals consist of correlated samples. Awdhesh Shukla, et al., [13] presented a high-capacity data-hiding method that combines lossless compression, advanced encryption standard, modified pixel value differencing and least significant bit substitution to achieve enhanced security against regular/ singular (RS) steganalysis.

Sun et al. [14] proposed Dual RSA which is the modified variant of RSA in order to decrease storage requirement. The output of key generation phase of proposed method has two distinct key pairs of RSA with identical private and public keys. Comparison of same with RSA is done based on security boundaries with trade-off between two algorithms. The paper [15] focuses on enhancing the security of RSA. Drawback of RSA is solved by using fake modulus instead of 'n'. Factorization of fake modulus 'Fn' is worthless. The proposed method increases the plain text limit. Computation cost to find original modulus using fake modulus is more.

To increase the implementation speed of RSA the authors of paper [16], proposed storage of keys in offline database known as RSA-key Generation offline. Implementation includes offline generation of keys and online encrypting and decrypting of messages. Using Decryption time is faster in offline RSA key generation rather than online RSA key generation for different key lengths.

The authors in paper [17] implemented new algorithm using two asymmetric crypto algorithms – RSA and Diffie- Hellman. The public key and private key generated from RSA is given as input to Diffie-Hellman algorithm. Same Session key (K) is used both for encrypting and decrypting of message using XOR function for secure transmission.

The authors of paper [18] used Pell's equation along with RSA for key generation method. Calculation of modulus (n), e and d parameter is same as that of RSA whereas public and private is different from RSA. The algorithm is safe from any attacks of RSA and security is increased. The parameter "d" is above the Weiner range.

3. Conclusion

Digital transmission of data has helped the human race in many ways and is creating lot of security issues as well, in this paper various techniques over cryptography, steganography and digital watermarking have been discussed out and it can be deduced that the need of cryptography and other data hiding algorithms is high but there should be a method which can follow the concept of cryptography, steganography and digital watermarking simultaneously.

References

[1] Yinghui Zhang, Dong Zheng and Robert H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," IEEE Internet of Things Journal, Vol. 5, No. 3, June 2018.

[2] Zhen Wang, Zhaofeng Ma,Shoushan Luo and Hongmin Gao," Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network Systems," IEEE Access,Special Section On Privacy Preservation For Large-Scale User Data In Social Networks,Vol. 6, March 2018.

[3] Abid Mehmood, Iynkaran Natgunanathan,Yong Xiang, Howard Poston, And Yushu Zhang,"Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications" IEEE Access, Vol. 6,July 2018.

[4] Kan Yang, Zhen Liu, Xiaohua Jia and Xuemin Sherman Shen,"Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach," IEEE Trans. on Multimedia, vol. 18, no. 5, May 2016.

[5] Jiguo Li, Wei Yao, Jinguang Han, Yichen Zhang and Jian Shen," User Collision Avoidance CP-ABE with Efficient Attribute Revocation for Cloud Storage," IEEE Systems Journal, Vol. 12, No. 2, June 2018.

[6] Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong, "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage," IEEE Transactions on Information Forensics and Security, Vol. 13, No. 8, August 2018.

[7] Jianting Ning, Zhenfu Cao,Xiaolei Dong,Kaitai Liang, Hui Ma and Lifei Wei, "Auditable σ-Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing," IEEE Transactions On Information Forensics And Security, Vol. 13, No. 1, January 2018.

[8] Sheng ding, Chen li and Hui li,"A Novel Efficient Pairing-free CP-ABE Based On Elliptic Curve Cryptography,"IEEE Access Special Section on Security and Trusted Computing for Industrial Internet of Things, Volume 6, June 2018.

[9] Qiang Wang, Li Peng, Hu Xiong, Jianfei Sun, And Zhiguang Qin, "Ciphertext-Policy Attribute-Based Encryption with Delegated Equality Test in Cloud Computing,"IEEE Access, Volume 6, February 2018.

[10] Jianghong Wei, Wenfen Liu, and Xuexian Hu," Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage," IEEE Systems Journal, Vol. 12, No. 2, June 2018.

[11] Shuming Qiu, Guoai Xu, Haseeb Ahmad and Licheng Wang," A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems," IEEE Access, Volume 6, March 2018.

[12] Sorina Dumitrescu and Xiaolin Wu, "A New Framework of LSB Steganalysis of Digital Media," IEEE Transactions On Signal Processing, Vol. 53, No. 10, October 2015.

[13] Awdhesh Shukla, Akanksha Singh, Balvinder Singh and Amod Kumar," A Secure and High-Capacity Data-Hiding Method Using Compression, Encryption and Optimized Pixel Value Differencing", IEEE Access,Vol. 6,October 2018

[14] H. M. Sun, M. E. Wu, W. C. Ting and M. J. Hinek, "Dual RSA and Its Security Analysis," in IEEE Transactions on Information Theory, vol. 53, no. 8, pp. 2922-2933, Aug. 2007.

[15] "Enhancing security features in RSA cryptosystem," 2012 IEEE Symposium on Computers & Informatics (ISCI), Penang, 2012, pp. 214-217.

[16] S. A. Nagar and S. Alshamma, "High speed implementation of RSA algorithm with modified keys exchange," 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Sousse, 2012, pp. 639-642.

[17] S. Gupta and J. Sharma, "A hybrid encryption algorithm based on RSA and Diffie-Hellman," 2012 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, 2012, pp. 1-4.

[18] T. C. Segar and R. Vijayaragavan, "Pell's RSA key generation and its security analysis," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, 2013, pp. 1-5.