A SECURE DATA TRANSFER METHOD USING A COMBINED CRYPTOGRAPHYAND STEGANOGRAPHY ALGORITHM

ALA SALEH KHALID TAHER

MASTER OF INFORMATION TECHNOLOGY
INFRASTRUCTURE UNIVERSITY KUALA LUMPUR
(IUKL)
2017

A SECURE DATA TRANSFER METHOD USING A COMBINED RYPTOGRAPHY AND STEGANOGRAPHY ALGORITHM

By

ALA SALEH KHALID TAHER

A Project Paper Submitted in Partial Fulfillment as the Requirement for the Master of Information Technology by Coursework in Faculty of Creative Media and Innovative Technology

IUKL
2017

The project paper was submitted to the senate of Infrastructure University Kuala Lumpur (IUKL) and has been accepted as partial fulfillment of the requirement for the degree of Master of Information Technology.

A SECURE DATA TRANSFER METHOD USING A COMBINED RYPTOGRAPHY AND STEGANOGRAPHY ALGORITHM

By

ALA SALEH KHALID TAHER

JUN 2017

Chair: Dr. Mohammed Awadh Ben Mubarak

Faculty: Faculty of Creative Media and Innovative Technology

During last decades, needs for cryptographic applications had increased exponentially. Civil encryption applications (banking, telecommunications, computers, credit cards, etc) become a fundamental engine of progress. The generalization of computers can provide much more complex algorithms for cryptography, however at the same time attacks can be automated. Theoretical progress is also made in the field of cryptography, with the invention of public key cryptography, which solves the problem of key exchange**.** However no matter how good is the cryptography algorithm, there is always a gape on it, or it is possible to break it with a powerful computer. Therefore in this study we propose to combine cryptography with steganography to secure data transfer between two applications. In addition two encryption algorithms (RC4 and Triple DES) will be investigated and compared. The idea is to use two levels of security. In the first step, the data is crypt using the stat of the art cryptography algorithms. Then the resulting cryptic code will be hidden in an image then transferred over the wire to the destination. The main advantage of this method is that the steganography will be strengthen by the cryptography algorithm because it is much easier to detect a plan text rather than a cryptic code as the words of a plan text are part of a language thus easily

recognizable. Furthermore, the hacker need to guess that the information is hidden in the image, then break the steganography protection then break the cryptography algorithm, thus this combination of steganography and cryptography will make the data transfer much more secure.

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful.

foremost praise be to Almighty Allah for all his blessings for giving me patience and good health throughout the duration of this master project.

To the one who taught me patience and success.

To whom I have lost him in the face of difficulties.

And did not stay alive until he sees what he wish ... my Father Allah forgive him.

"Who taught me to hold whatever circumstances changed .... My dear mother.

To my wonderful wife, who sacrificed everything and stood beside me in this way, she was a best help to me in my journey.

And to my dear children.

I would like to express my gratitude to my supervisor Dr. Mohammed Awadh Ben Mubarak for the useful comments , remarks and constant support. and I would also like to thank the examiner Dr. Abudhahir Buhari .

And finally , I would like to thank all my family and friends for their support.

APPROVAL

The project paper was submitted to the senate of Infrastructure University Kuala Lumpur (IUKL) and has been accepted as partial fulfillment of the requirement for the degree of Master of Information Technology. the members of the project examination committee were as following:

Dr. Mohammed Awadh Ben Mubarak

Faculty: Creative Media and Innovative technology

University: Infrastructure University Kuala Lumpur (IUKL)

Supervisor

DR. Abudhahir Buhari

Faculty: Creative Media and Innovative technology

University Infrastructure University Kuala Lumpur (IUKL)

Examiner

(Assoc. Prof. Dr. Manal Mohsen Abood, PhD

Director

Center for postgraduate Studies

Infrastructure University Kuala Lumpur (IUKL)

Date

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. In addition, I declare that it has not been previously, and it is not concurrently, submitted for any other degree at Infrastructure University Kuala Lumpur or at any other institutions.

Signature: …….

Name: ALA SALEH KHALID TAHER

Date: 20th March.2017

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction

The rapid development of communication and transmission facilities, including the development of the Internet and high-speed networks, has facilitated access to information in general. The dissemination and sharing of digital data has become very easy and wide-ranging. Of course, this can only be beneficial because access to information has become instantaneous. On the other hand, the problem of security arises more and more. Indeed, data sharing servers, P2P networks have opened a very wide field to dishonest users to manipulate information in an illegal way.

Therefore, this study proposes to reinforce this confidentiality of the data during transfer and obtain rigorous authentication, thus we will insert a cryptology using the RC4 and Triple DES algorithms into the steganography process done using least significant bit (LSB) algorithm.

1.1.1 RC4 Cryptography

RC4 (Rivest Cipher 4) is a floating cipher algorithm designed in 1987 by Ronald Rivest, one of the inventors of the RSA, for RSA Laboratories. It is supported by different standards, for example in TLS (formerly SSL). Officially named Rivest Cipher 4, the acronym RC is also nicknamed Ron's Code as in the case of RC2, RC5 and RC6 (Akgün, Kavak, & Demirci, 2008, p. 4).

RC4's details were initially kept secret but in 1994 a description of the encryption was posted anonymously on the Cypherpunks (Paterson & Strefler, 2015) mailing list. The message then appeared on the sci.crypt 2 forum and then on various sites.

REFERENCES

Abdalla, F. M., & Mohammed, A. E. (2016). DES Security Enhancement using Genetic Algorithm. Retrieved from http://repository.sustech.edu/handle/123456789/16646

Abikoye Oluwakemi, C., Adewole Kayode, S., & Oladipupo Ayotunde, J. (2012). Efficient data hiding system using cryptography and steganography. *IJAIS*, *11*(4), 1-6.

Akgün, M., Kavak, P., & Demirci, H. (2008). New Results on the Key Scheduling Algorithm of RC4. In *INDOCRYPT* (Vol. 8, pp. 40–52). Springer. Retrieved from http://link.springer.com/content/pdf/10.1007/978-3-540-89754-5.pdf#page=52

Al-Haj, A., & Mohammad, A. (2010). Digital audio watermarking based on the discrete wavelets transform and singular value decomposition. *European Journal of Scientific Research*, *39*(1), 6–21.

Asrani, A., Koul, V., & Khot, R. (2016). Review of Network Steganography Techniques. *Imperial Journal of Interdisciplinary Research*, *2*(12). Retrieved from http://www.imperialjournals.com/index.php/IJIR/article/view/3059

Aung, P. P., & Naing, T. M. (2014). A novel secure combination technique of steganography and cryptography. *International Journal of Information Technology, Modeling and Computing (IJITMC)*, *2*(1), 55–62.

Barker, B., & Smith, M. (2015). Hash Functions Based on Data Encryption Standard (DES). Retrieved from http://scholarworks.boisestate.edu/as_15/43/

Britz, M. T. (2009). *Computer Forensics and Cyber Crime: An Introduction, 2/E*. Pearson Education India.

Chen, B., & Wornell, G. W. (1999). An information-theoretic approach to the design of robust digital watermarking systems. In *Acoustics, Speech, and Signal Processing, 1999. Proceedings., 1999 IEEE International Conference on* (Vol. 4, pp. 2061–2064). IEEE. Retrieved from http://ieeexplore.ieee.org/abstract/document/758336/

Dharwadkar, N. V., Amberker, B. B., & Gorai, A. (2011). Non-blind watermarking scheme for color images in RGB space using DWT-SVD. In *Communications and Signal Processing (ICCSP), 2011 International Conference on* (pp. 489–

493). IEEE. Retrieved from http://ieeexplore.ieee.org/abstract/document/5739368/

Feiten, L., & Sauer, M. (2015). Extracting the RC4 secret key of the Open Smart Grid Protocol (OSGP). Retrieved from https://www.acsac.org/2015/workshops/icss/Linus%20feiten-slides.pdf

Garg, S., Garg, T., & Mallick, B. (2017). Secure Message Transfer using Triple DES. *International Journal of Computer Applications*, *165*(8). Retrieved from http://search.proquest.com/openview/7cee17d18d275bc846ae74a96efefea7/1?pq-origsite=gscholar&cbl=136216

Holub, V., & Fridrich, J. J. (2014). Challenging the doctrines of JPEG steganography. In *Media Watermarking, Security, and Forensics* (p. 902802). Retrieved from http://opticalengineering.spiedigitallibrary.org/pdfaccess.ashx?url=/data/conferences/spiep/77655/902802.pdf

Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.364.3275

Jhaveri, M. H., Cetin, O., Gañán, C., Moore, T., & Eeten, M. V. (2017). Abuse reporting and the fight against cybercrime. *ACM Computing Surveys (CSUR)*, *49*(4), 68.

Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography*. CRC press. Retrieved from https://books.google.com/books?hl=en&lr=&id=OWZYBQAAQBAJ&oi=fnd&pg=PR2&dq=Introduction+to+modern+cryptography&ots=BbtiwPU-6j&sig=RXZPoGKNsHPyHj3h2bzWw9ldAQk

Kumar, S., Yadav, S., & Kumar, D. (2017). Secured Communication using Data Dictionary through Triple DES. *International Journal of Computer Applications*, *166*(3). Retrieved from http://search.proquest.com/openview/1c06b2c6a065cd477406c12e5fa57f5b/1?pq-origsite=gscholar&cbl=136216

Lai, C.-C., & Tsai, C.-C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement*, *59*(11), 3060–3063.

Liu, K.-C., & Chou, C.-H. (2009). Robust and transparent watermarking scheme for colour images. *IET Image Processing*, *3*(4), 228–242.

Lou, D.-C., & Hu, C.-H. (2012). LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis. *Information Sciences*, *188*, 346–358.

Mansouri, A., Aznaveh, A. M., Torkamani-Azar, F., & Kurugollu, F. (2010). A low complexity video watermarking in H. 264 compressed domain. *IEEE Transactions on Information Forensics and Security*, *5*(4), 649–657.

Mao, W. (2013). The role and effectiveness of cryptography in network virtualization: a position paper. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security* (pp. 179–182). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2484337

Masram, R., Shahare, V., Abraham, J., & Moona, R. (2014). Analysis and comparison of symmetric key cryptographic algorithms based on various file features. *International Journal of Network Security & Its Applications*, *6*(4), 43.

Menezes, A. J. (2012). *Elliptic curve public key cryptosystems* (Vol. 234). Springer Science & Business Media. Retrieved from https://books.google.com/books?hl=en&lr=&id=QE7hBwAAQBAJ&oi=fnd&pg=PR9&dq=Elliptic+curve+public+key+cryptosystems&ots=ZcleByjHLr&sig=Mwruihxf8rnvyC5mLA-t49y0Brs

Moskowitz, S. A. (2006). *Optimization methods for the insertion, protection, and detection of digital watermarks in digital data*. Google Patents. Retrieved from https://www.google.com/patents/US7107451

Nene, S. A., Nayar, S. K., Murase, H., & others. (1996). Columbia object image library (coil-20). Retrieved from https://pdfs.semanticscholar.org/ca68/91667e2cf6c950c3c8f8ea93e55320173505.pdf

Pappas, T. N., Safranek, R. J., & Chen, J. (2000). Perceptual criteria for image quality evaluation. *Handbook of Image and Video Processing*, 669–684.

Patel, G. R., & Panchal, K. (2014). Hybrid Encryption Algorithm. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.687.5556

Paterson, K. G., & Strefler, M. (2015). A Practical Attack Against the Use of RC4 in the HIVE Hidden Volume Encryption System. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (pp. 475–482). New York, NY, USA: ACM. https://doi.org/10.1145/2714576.2714596

Pröfrock, D., Schlauweg, M., & Müller, E. (2006). Video watermarking by using geometric warping without visible artifacts. In *International Workshop on*

Information Hiding (pp. 78–92). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-74124-4_6

Rajyaguru, M. H. (2012). CRYSTOGRAPHY-Combination of Cryptography and Steganography with Rapidly Changing Keys. *Int J Emerg Technol Ad Eng*, *2*(10), 329–332.

Reed, A., & Hannigan, B. (2006). *Watermark detection using adaptive color projections*. Google Patents. Retrieved from https://www.google.com/patents/US7072487

Rice, J. R. (2016). *Methods, systems, and computer readable media for preventing software piracy and protecting digital documents using same*. Google Patents. Retrieved from https://www.google.com/patents/US9275203

Santra, A. K., & Nagarajan, S. (2013). A Modified DES and Triple DES Algorithm for Wireless Networks. *International Journal of Computer Science and Network Security (IJCSNS)*, *13*(4), 44.

Saraireh, S. (2013). A Secure Data Communication system using cryptography and steganography. *International Journal of Computer Networks & Communications*, *5*(3), 125.

Singh, A., & Malik, S. (2013). Securing data by using cryptography with steganography. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5). Retrieved from https://pdfs.semanticscholar.org/fbd8/fce8985c12b3d76ed251c31beab6fd3762fb.pdf

Singh, P., & Chadha, R. S. (2013). A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, *2*(9), 165–175.

Singh, S. P., & Maini, R. (2011). Comparison of data encryption algorithms. *International Journal of Computer Science and Communication*, *2*(1), 125–127.

Suryakant, P. V., Bhosale, R. S., & Panhalkar, A. R. (2012). A novel security scheme for secret data using cryptography and steganography. *International Journal of Computer Network and Information Security*, *4*(2), 36.

Topkara, U., Topkara, M., & Atallah, M. J. (2006). The hiding virtues of ambiguity: quantifiably resilient watermarking of natural language text through synonym substitutions. In *Proceedings of the 8th workshop on Multimedia and security* (pp. 164–174). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1161397

Usha, S., Kumar, G. S., & Boopathybagan, K. (2011). A secure triple level encryption method using cryptography and steganography. In *Computer science and network technology (ICCSNT), 2011 international conference on* (Vol. 2, pp. 1017–1020). IEEE. Retrieved from http://ieeexplore.ieee.org/abstract/document/6182134/

Xuehua, J. (2010). Digital watermarking and its application in image copyright protection. In *Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on* (Vol. 2, pp. 114–117). IEEE. Retrieved from http://ieeexplore.ieee.org/abstract/document/5523112/

Yar, M. (2013). *Cybercrime and society*. Sage. Retrieved from https://books.google.com/books?hl=en&lr=&id=Ye4QAAAAQBAJ&oi=fnd&pg=PP2&dq=Cybercrime+and+society&ots=cPEkuYS_nG&sig=QdoaM3THVXJOWLqIiw4kykK1p0k

Young, H. (2016). Ultrasonic Data Transmission and Steganography. Retrieved from http://digitalcommons.kennesaw.edu/honors_etd/6/

Yuan, J., & Chen, H. (2014). Embedding Suitability Adaptive Cover Selection for Image Steganography. In *International Conference on e-Education, e-Business and Information Management, IEEE* (pp. 36–40). Retrieved from https://www.researchgate.net/profile/Haishan_Chen5/publication/266647387_Embedding_Suitability_Adaptive_Cover_Selection_for_Image_Steganography/links/57a495dc08ae455e8538ee78.pdf

Zúquete, A. (2016). Exploitation of Dual Channel Transmissions to Increase Security and Reliability in Classic Bluetooth Piconets. In *Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks* (pp. 55–60). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2988275