A NOVEL IMAGE AUTHENTICATION AND RIGHTFUL OWNERSHIP DETECTION FRAMEWORK BASED ON DWT WATERMARKING IN CLOUD ENVIRONMENT

REZA KHALEGHPARAST

UNIVERSITI TEKNOLOGI MALAYSIA

PSZ 19:16 (Pind. 1/07)

UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name: REZA KHALEGHPARAST

Date of birth : 21 MARCH 1987

Title : A NOVEL IMAGE AUHTNETICATION AND RIGHTFUL OWNERSHIP DETECTION FRAMEWORK BASED ON DWT WATERMARKING IN CLOUD ENVIRONMENT

Academic Session: 2012/2013

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

☑ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

Declare that this thesis is classified as:

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange. Certified by:

SIGNATURE	**SIGNATURE OF SUPERVISOR**
(NEW IC NO. /PASSPORT NO.) F19845193	**NAME OF SUPERVISOR** PROF. DR. AZIZAH ABD MANAF
Date: JANUARY 2013	Date: JANUARY 2013

NOTES: * If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.

"I declare that I have read this project, in my
opinion this project report has satisfied the scope and quality for the
award of the degree of master of Computer Science (Information Security)."

Signature :

Name of Supervisor : Prof. Dr. Azizah Abd Manaf

Date : JANUARY 2013

A NOVEL IMAGE AUTHENTICATION AND RIGHTFUL OWNERSHIP DETECTION FRAMEWORK BASED ON DWT WATERMARKING IN CLOUD ENVIRONMENT

REZA KHALEGHPARAST

A thesis submitted in partial fulfillment of

the requirements for the award of the

Master of Computer Science (information security)

Advanced Informatics Schools

Universiti Teknologi Malaysia

January 2013

I declare that this project report entitled "A Novel Image Authentication and Rightful Ownership Detection Framework Based on DWT Watermarking in Cloud Environment" is the result of my own research except as cited in the references. The project report has not been accepted for any degree and is not concurrently submitted in the candidature of any other degree.

SIGNATURE:

Name : REZA KHALEGHPARAST

Date : JANUARY 2013

ACKNOWLEDGEMENT

First, thank you Allah for giving me strength to take up this challenge and with your blessing to complete this study. Second and foremost, I am deeply indebted to my supervisor, Prof. Dr. Azizah Abd Manaf for her patience in assisting, advising and guiding me throughout this project. To admin staff of UTM AIS, thank you for your continuous help and kind assistance during my presence in UTM AIS.

To my dear father, mother and also my little sister, a million thanks for your understanding and ardent support extended to me throughout my journey to accomplish this study. Last but not least I want to thank all of my friends especially all my dear classmates who helped and understood me during this project.

DECLARATION OF PROJECT STATUS FORM

Student Name : **REZA KHALEGHPARAST**

Student ID : **MC101226**

Supervisor Name : **Prof. Dr. Azizah Abd Manaf**

Course code : **MCU1016**

Academic : **Semester 3** **Year 2012/2013**

Title of Project : A NOVEL IMAGE AUTHENTICATION AND RIGHTFUL OWNERSHIP DETECTION FRAMEWORK BASED ON DWT WATERMARKING IN CLOUD ENVIRONMENT

The above project work *has / has not**** fulfilled the necessary criteria towards the completion of the project, hence the mentioned student is *ready / not ready**** to submit the project report and orally present his/her project work.

*** **Additional Remarks**

_____

SUPERVISOR'S SIGNATURE

Date :

***Choose appropriately

This form MUST be submitted a week before the drop date in the UTM academic calendar.

ABSTRACT

Cloud computing has been highlighted by many organizations because of its benefits to use it anywhere. Efficiency, Easy access information, quick deployment, and a huge reduce of cost of using it, are some of the cloud advantages. While cost reduction is one of the great benefits of cloud, privacy protection of the users' data is also a significant issue of the cloud that cloud providers have to consider about. This is a vital component of the cloud's critical infrastructure. Cloud users use this environment to enable numerous online transactions crossways a widespread range of sectors and to exchange information. Especially, misuse of the users' data and private information are some of the important problems of using cloud environment. Cloud untrustworthy environment is a good area for hackers to steal user's stored data by Phishing and Pharming techniques. Therefore, cloud vendors should utilize easy- to-use, secure, and efficient environment. Besides they should prepare a way to access cloud services that promote data privacy and ownership protection. The more data privacy and ownership protection in cloud environment, the more users will attract to use this environment to put their important private data. In this study, a rightful ownership detection framework has been proposed to mitigate the ownership protection in cloud environment. Best methods for data privacy protection such as image authentication methods, watermarking methods and cryptographic methods, for mitigating the ownership protection problem to use in cloud environment, have been explored. Finally, efficiency and reliability of the proposed framework have been evaluated and analyzed.

ABSTRAK

"Cloud Computing" ataupun teknologi perkomputeran telah digunakan oleh banyak organisasi kerana keboleh gunaannya yang meluas. Antara faktor-faktornya ialah kecekapanya, akses maklumat yang mudah, penggunaan yang cepat, dan yang paling penting dapat mengurangkan kos dengan wujudnya penggunaan fenomena "Cloud Computing" yang mana adalah satu kelebihan.Walaupun pengurangan kos adalah salah satu faedah besar, melindungi privasi data pengguna adalah juga suatu yang penting yang mana para pemaju "Cloud Computing" perlu untuk memandang serius. Ini adalah satu komponen penting dalam infrastruktur kritikal "Cloud Computing". Pengguna perlu menggunakan persekitaran ini untuk membolehkan pelbagai transaksi dalam talian merentasi pelbagai sektor dan dapat bertukar-tukar maklumat. Perlu di ambil perhatian dalam penyalahgunaan data pada pengguna dan maklumat peribadi adalah beberapa masalah yang perlu diambil berat dalam menggunakan persekitaran ini. "Cloud Computing" yang tidak boleh dipercayai menjadi tumpuan bagi hacker untuk aktiviti menceroboh data pengguna yang disimpan dengan cara Phishing dan Pharming. Oleh itu, vendor "Cloud" perlu menyediakan perkhidmatan yang mesra pengguna, selamat, dan persekitaran yang cekap. Selain itu juga perlu menyediakan satu cara untuk mengakses perkhidmatan yang meningkatkan privasi suatu data dalam melindungi pengguna. Data yang lebih privasi dan dilindungi, dalam persekitaran "Cloud Computing" dapat menarik lebih ramai pengguna untuk menggunakan persekitaran ini dengan yakin dalam menjagai privasi suatu data. Dalam kajian ini, rangka kerja mengesan pemilik yang sah telah dicadangkan untuk melindungi pengguna dalam persekitaran awan. Kaedah yang paling berkesan untuk merlindungi data privasi adalah seperti kaedah pengesahan imej, "Watermarking" dan "kriptografi", untuk mengurangkan risiko pada penguna dalam persekitaran "cloud", yang mana telah dapat diatasi. Akhirnya, kecekapan dan kebolehpercayaan rangka kerja yang dicadangkan tersebut telah dinilai dan dianalisis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATION	TITLE
ISCH	Image Similarity Checking
WECH	Watermark Existence Checking
CFDH	Cloud Fix password, Dynamic password, Hash
DYN	Dynamic
HECH	Hash Existence Check
DWT	Discrete Wavelet Transformation

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

With the dramatic development of technology, computer and its usage have been changed among people and improved all over the world in the last few years. Introducing Cloud computing as a new technology publicly making it the next generation of technologies. Cloud service providers have made tangible progress in securing their environments and protecting customer instances. But how do organizations maintain direct control of their data processed by cloud service providers is the question that highlights the importance of a clear breakdown of roles and responsibilities between cloud service providers and customers when moving sensitive and proprietary data to third-party service providers. Maintaining control and ownership of data in the cloud and the role of encryption in use it, is one of the main concerns of the cloud providers (Liu *et al.*, 2011b; Yuhan and En-hui, 2009).

1.1.1 Definition of Cloud Computing

Cloud computing is a general term for something which is involved delivering hosted services over the Internet. These services can be divided into three categories, Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The name cloud computing was inspired by the cloud symbol that is often used to represent the Internet in diagrams or tables (Computing, 2007).

1.1.2 Layers of cloud computing

Infrastructure as a Service (IaaS) brings computer infrastructure, usually a platform virtualization environment as a service. One of the important options, which are broadly used in IaaS is virtualization in order to integrate/decompose physical resources in an ad-hoc method. An example of IaaS can be an Amazon's EC2. (Dillon *et al.*, 2010)

Platform as a Service (PaaS) come up with a computing platform or solution as a service. It facilitates positioning of applications, which has been used in the cloud without any cost and complexity of paying any money or managing the underlying hardware and software layers. Google Application Engine can be an example of PaaS (Dillon *et al.*, 2010).

Software as a Service (SaaS) comes with software as a service over the World Wide Web, excluding the need to install and run the application Cloud through three networks from different clients by application users. Some example of using SaaS is Google docs or sales force (Dillon *et al.*, 2010).

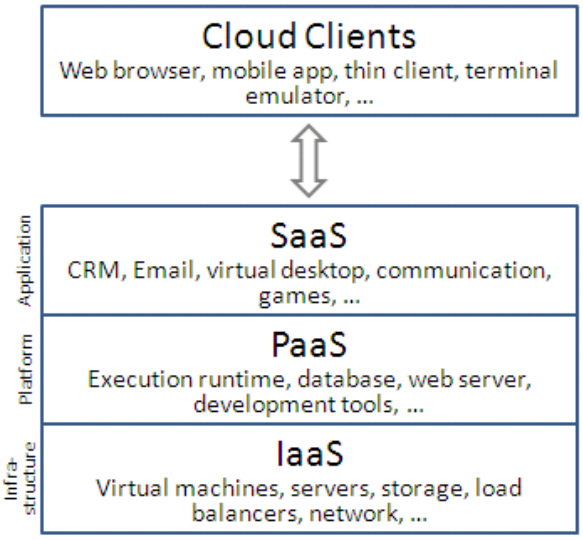

Figure 1.1: Cloud Computing Layers

1.1.3 Security Definition of Cloud Computing

One of the important issues of cloud computing is loss of control, for example, users of a particular service does not know the storage and processed place of his data. Data and their computation can be migrated from place to place which cannot be control of service users. Data can be freely cross the physical borders and it can become a threat to itself. Another example of losing control is that the cloud providers get paid for a service which they run and have no information about the details (Lombardi and Di Pietro, 2011).

Security of Cloud computing has been enhanced in many ways, but still needs cooperation to give more trust to its users. Security over cloud environment is important for those who are about to use their critical information over it. Different methods have been used during the last few years to improve the security of cloud (Lombardi and Di Pietro, 2011). One of these methods that have been used in the cloud security area is watermarking.

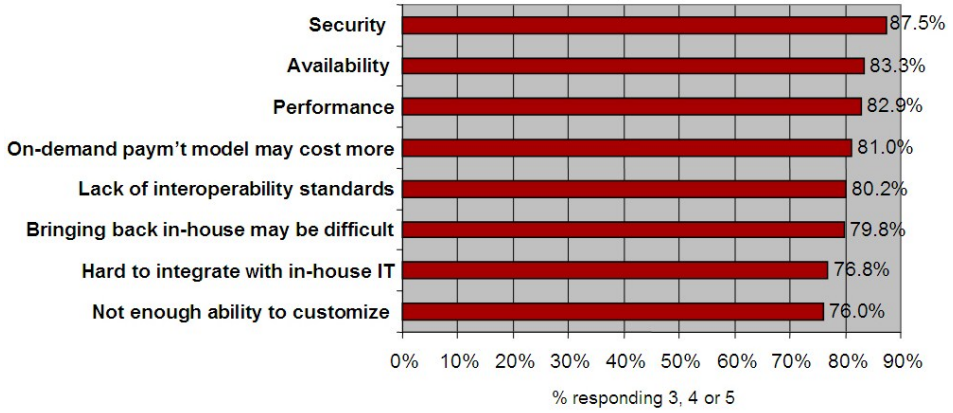

Figure 1.2: IDC Enterprise Panel (2008)

1.1.4 Principles of Watermarking

Watermarking is a technology for copyright protection, which has been pushed in the traditional copyright protection to the digital one to avoid being illegally copied or tampered. The major idea of the watermarking is to introduce small patterns in the data that want to be watermarked without changing the original source. If there is any illegal copy of the original data occurred, the real owner of data can verify his ownership of that data (Liu *et al.*, 2011b).

1.2 Background of the problem

Illegal copying, tampering, and other violations on digital products are increasingly spread every day. Cloud computing systems are introducing a new method which leads people to come out from the small world of personal computers to the world of internet, running on a large number of distributed computers. "Cloud" denotes to all kinds of the computing center distributed on the Internet which containing thousands of computers or servers rather than purchase of high-performance hardware or the development of various features of the software, users can use any Internet-connected devices in connection to the "cloud", and processing and storing data in the "cloud" by using the software or services provided by cloud, but every technology has its own problems (Wang and Shao, 2012)

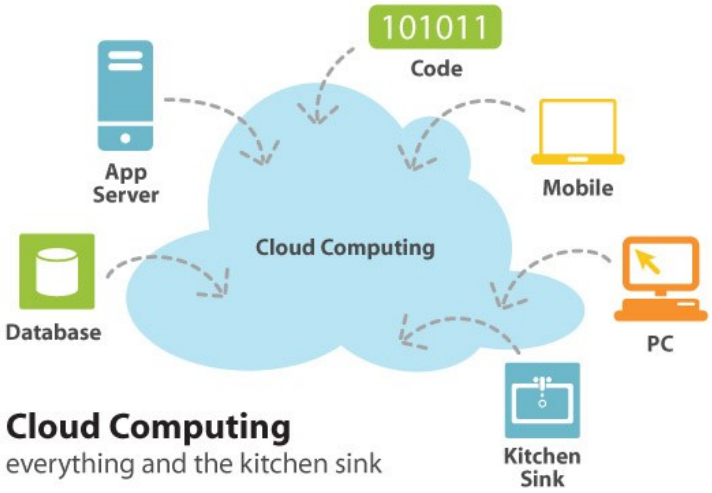

Figure 1.3: Cloud computing simple illustration

Internet connections have become a commodity product in many countries, and Internet-scale "cloud computing" has started to compete with traditional software business with its technological benefits and economy of scale, after decades of engineering development and infrastructural investment. Cloud computing is an Internet ware promising enabling technology. One of the most important distinctive characteristic of cloud computing is the global integration of data, logic, and users, but such integration enlarges concerns about privacy, that is one of the most regularly cited reasons mentioned by enterprises in order not to transfer to cloud-based solutions. It has been claimed that cloud-based systems should be consisted of privacy as a basic design goal, and that privacy in a cloud environment is bidirectional, covering not only end users but also the application providers. End users are required to have privacy aware software services, which could be able to prevent their private data from being revealed to other users or cloud providers. A privacy-protected testing methodology is needed for application providers to prevent the internal activities and product features of the company from being exposed to external users. The research challenges in this unique design space, and exploring potential solutions for improving privacy protection in many important system components has been discussed by focusing on privacy protection.

One of the biggest problems with cloud computing is security. Security is an important concern of every individual or organization, who wants to use cloud (Abbadi and Martin, 2011). There are so many researches about cloud security, but the gap still remains, because the cloud is a wide area (Asghar *et al.*, 2012; Rodero-Merino *et al.*, 2012; Sreenivas *et al.*, 2012; Wang and Shao, 2012).

In spite of the fact that cloud computing has high potential in decreasing costs and improving productivity, and is able to provide greater convenience and benefits to the customers, several experts seriously notify that many obstacles exist in cloud computing adoption and application. Indeed, many open questions have been put forth in cloud security, including customers' confidence in providers, privacy, security technologies and regulations. The issues of security raise several serious threats and challenges for cloud computing and its customers. On the one hand, some security technologies specifications and information management details should be provided by cloud providers, including the policy maker's qualifications, architects and coders, technical mechanisms and risk-control processes. On the other hand, it's better for customers to consider and raise their security requirements comprehensively, such as Confidentiality, customers' data Privacy and Integrity, before choosing a cloud service. Furthermore, customers' work copyright is also took to the consideration before a cloud be chosen by the customer. It is used to protect the original multimedia works authorship like images, audios and, videos. There are two key issues which should be considered and be resolved: first one is customers' works copyright and integrity protections, the other is how to identify if duty once customers' works are taken vent or modified.

The second major issue is about privacy, which originates from the fact that in cloud computing, data and programs are collected off-premises and would be managed by a service provider. When a third party can have access to your data, nobody knows what is going to be happened.

The essence of cloud computing is that a customer not only entrusts its own digital information, but also with that of third parties, to the cloud computing service

provider. Then the customer uses technology and information, which are stored in the cloud by the provider, to create further information. All these steps happen online, by using such technology which the customer has no control on it. Inevitably, ownership rights are affected. The researcher addresses three questions which have been shown their concerns about cloud ownership. First, what are the expectations of those involved in a cloud computing relationship about information ownership, and how closely does the current legal framework match those expectations? Second, Does cloud computing generate new types of information and if so how is that information owned? Third, how does the allocation of ownership in the terms of service of the major cloud computing providers deal with these issues?

According to Yang and Lin (2011), with the faster Internet method were used widely, digital image watermarking becomes a significant topic of intellectual property in the digital age. They propose a method that can process image watermarking based on a robust method, which combines the Singular Value Decomposition (SVD) and Distributed Discrete Wavelet Transformation (DDWT) on cloud environments.

In every data transaction and each network, one of the important problems is noise on data. In this project there is a need for robust watermark on the image which wants to transfer through the cloud environment. Noise problem will become an important issue to the watermarked image (Gien, 1978).

1.3 Problem Statement

The huge amount of personal information stored in the cloud has made it a target for attackers in getting valuable information. There are many attacks of different methods on a Cloud and attacks are still on-going (Gruschka and Jensen, 2010; Zhou *et al.*, 2011). Breaking the copyright rules in Cloud environments, especially in social networks are common, and this can be a huge vulnerability for cloud providers to find the original sources and their ownerships that will be a main and primary problem to consider about in this research (Hwang and Li, 2010).

1.4 Project Objectives

The objectives of this study are as below:

i. To investigate privacy and watermarking research methods on image authentication, which can be used and implement in the cloud environment.
ii. To propose and design a novel framework for enhancing the cloud image authentication by using the selected watermarking method according to the purpose of finding the rightful ownership.
iii. To test and evaluate the proposed framework in cloud to establish in the cloud environment.

1.5 Research Questions

The main questions of this research motivates to answer, are as follows:

i. What are the approaches for securing the ownership protection in private cloud by using the ownership protection rules under the watermarking methods?
ii. How to design a new framework to increase rightful ownership protection in a private cloud?
iii. How to evaluate the proposed framework in a private cloud?

1.6 Project Aim

The aim of this study is to find a way for enhancing the cloud ownership protection by using an appropriate privacy protection and watermarking methods on image files in cloud environment. First, the appropriate method will find. Next is to implement the method by simulating it in cloud environment.

1.7 Scope of the Study

The scope of this study is to examine the existing privacy protection methods and watermarking algorithms for image watermarking and find the appropriate method to implement in cloud environment to increase the copyright protection and ownership detection in cloud environment.

REFERENCES

Abbadi, I. M., and Martin, A. (2011). Trust in the Cloud.

Allan M. Bruce Department of Engineering, U. o. A. (2001). A review of watermarking

Asghar, M. R., Ion, M., Russello, G., and Crispo, B. (2012). Securing data provenance in the cloud. *IFIP WG 11.4 International Workshop on Open Problems in Network Security, iNetSec 2011, June 9, 2011 - June 9, 2011*. Lucerne, Switzerland: 145-160.

Bangaleea, R., and Rughooputh, H. (2002). Performance improvement of spread spectrum spatial-domain watermarking scheme through diversity and attack characterisation 293-298 vol. 291.

Cayre, F., Fontaine, C., and Furon, T. (2005). Watermarking security: theory and practice. *Signal Processing, IEEE Transactions on.* 53(10), 3976-3987.

Chandra, D. V. S. (2002). Digital image watermarking using singular value decomposition. *Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on*. 4-7 Aug. 2002 III-264-III-267 vol.263.

Chang, C.-C., Hu, Y.-S., and Lin, C.-C. (2007). *A Digital Watermarking Scheme Based on Singular Value Decomposition*

Combinatorics, Algorithms, Probabilistic and Experimental Methodologies. In B. Chen, M. Paterson and G. Zhang (Eds.), (Vol. 4614, pp. 82-93): Springer Berlin / Heidelberg.

Chang, C. Y., Wang, H. J., and Su, S. J. (2010). Copyright authentication for images with a full counter-propagation neural network. *Expert Systems with applications.* 37(12), 7639-7647.

Chuhong, F., Kundur, D., and Kwong, R. H. (2006). Analysis and design of secure watermark-based authentication systems. *Information Forensics and Security, IEEE Transactions on.* 1(1), 43-55.

Computing, S. C. (2007). Definition of cloud computing. from http://searchcloudcomputing.techtarget.com/definition/cloud-computing

Dillon, T., Wu, C., and Chang, E. (2010). Cloud computing: Issues and challenges. *24th IEEE International Conference on Advanced Information Networking and Applications, AINA2010, April 20, 2010 - April 23, 2010*. Perth, WA, Australia: 27-33.

Gao, T., Gu, Q., and Emmanuel, S. (2009). A novel image authentication scheme based on hyper-chaotic cell neural network. *Chaos, Solitons & Fractals.* 42(1), 548-553.

Gien, M. (1978). A File Transfer Protocol (FTP). *Computer Networks (1976).* 2(4–5), 312-319.

Gruschka, N., and Jensen, M. (2010). Attack surfaces: A taxonomy for attacks on cloud services 276-279.

Gu, L., and Cheung, S. C. (2009). Constructing and testing privacy-aware services in a cloud computing environment: challenges and opportunities 2.

Hernandez Martin, J. R., and Kutter, M. (2001). Information retrieval in digital watermarking. *Communications Magazine, IEEE.* 39(8), 110-116.

Huang, C. H., and Wu, J. L. (2004). Attacking visible watermarking schemes. *Multimedia, IEEE Transactions on.* 6(1), 16-30.

Hwang, K., and Li, D. (2010). Trusted cloud computing with secure resources and data coloring. *Internet Computing, IEEE.* 14(5), 14-22.

Jing, Z., Anthony, T. S. H., Gang, Q., and Pina, M. (2007). Robust Video Watermarking of H.264/AVC. *Circuits and Systems II: Express Briefs, IEEE Transactions on.* 54(2), 205-209.

Johnson, N. F., Duric, Z., Jajodia, S., and Memon, N. (2001). Information Hiding: Steganography and Watermarking—Attacks and Countermeasures. *Journal of Electronic Imaging.* 10, 825.

Jong Won, S., and Jin Woo, H. (2001). Audio watermarking for copyright protection of digital audio data. *Electronics Letters.* 37(1), 60-61.

Kirovski, D., and Malvar, H. S. (2003). Spread-spectrum watermarking of audio signals. *Signal Processing, IEEE Transactions on.* 51(4), 1020-1033.

Kuttera, M., Voloshynovskiya, S., and Herrigela, A. (2000). The watermark copy attack. *Security and watermarking of multimedia contents II: 24-26 January, 2000, San Jose, California.* 3971, 371.

Li, D. (2004). Artificial intelligence with uncertainty 2-2.

Liu, Y.-C., Ma, Y.-T., Zhang, H.-S., Li, D.-Y., and Chen, G.-S. (2011a). A method for trust management in cloud computing: Data coloring by cloud watermarking. *International Journal of Automation and Computing.* 8(3), 280-285.

Liu, Y. C., Ma, Y. T., Zhang, H. S., Li, D. Y., and Chen, G. S. (2011b). A method for trust management in cloud computing: Data coloring by cloud watermarking. *International Journal of Automation and Computing.* 8(3), 280-285.

Lombardi, F., and Di Pietro, R. (2011). Secure virtualization for cloud computing. *Journal of Network and Computer Applications.* 34(4), 1113-1122.

O'Ruanaidh, J. J. K., Dowling, W. J., and Boland, F. M. (1996). Watermarking digital images for copyright protection. *Vision, Image and Signal Processing, IEE Proceedings* -. 143(4), 250-256.

Rodero-Merino, L., Vaquero, L. M., Caron, E., Muresan, A., and Desprez, F. (2012). Building safe PaaS clouds: A survey on security in multitenant software platforms. Langford Lane, Kidlington, Oxford, OX5 1GB, United Kingdom: 96-108.

Sherekar, S., Thakare, V., and Jain, S. (2008). Role of Digital Watermark in e-governance and e-commerce. *International Journal of Computer Science and Network Security.* 8(1), 257-261.

Sherekar, S., Thakare, V., Jain, S., Miss Ashwini, D. B., Tijare, P., Deshpande, M. S. A., et al. (2011). Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks. *International Journal Of Computer Science And Applications.* 4(2).

Sreenivas, V., ArunaKumari, B., and VenkataRao, J. (2012). Enhancing the security for information with virtual data centers in cloud. *2011 International Conference on Future Wireless Networks and Information Systems, ICFWI 2011, November 30, 2011 - December 1, 2011*. Macao, China: 277-282.

Tan, X., and Ai, B. (2011). The issues of cloud computing security in high-speed railway 4358-4363.

Wang, K., and Shao, Q. (2012). Analysis of cloud computing and information security. *2nd International Conference on Frontiers of Manufacturing and Design Science, ICFMD 2011, December 11, 2011 - December 13, 2011*. Taichung, Taiwan: 3810-3813.

Yang, C.-T., Lin, C.-H., and Chang, G.-L. (2011a). Implementation of image watermarking processes on cloud computing environments. *2nd International Conference on the Emerging Areas of Security-Enriched Urban Computing and Smart Grids, SUComS 2011, September 21, 2011 - September 23, 2011*. Hualien, Taiwan: 131-140.

Yang, C. T., Lin, C. H., and Chang, G. L. (2011b). Implementation of Image Watermarking Processes on Cloud Computing Environments. *Security-Enriched Urban Computing and Smart Grid*, 131-140.

Yu, Z., Wang, C., Thomborson, C., Wang, J., Lian, S., and Vasilakos, A. V. (2011). A novel watermarking method for software protection in the cloud.

Yuhan, Z., and En-hui, Y. (2009). Joint robust watermarking and compression using variable-rate scalar quantization. *Information Theory, 2009. CWIT 2009. 11th Canadian Workshop on*. 13-15 May 2009 183-186.

Zander, S., Armitage, G., and Branch, P. (2007). A survey of covert channels and countermeasures in computer network protocols. *Communications Surveys & Tutorials, IEEE*. 9(3), 44-57.

Zhao, X., and Ho, A. (2010). *An Introduction to Robust Transform Based Image Watermarking Techniques*

Intelligent Multimedia Analysis for Security Applications. In H. Sencar, S. Velastin, N. Nikolaidis and S. Lian (Eds.), (Vol. 282, pp. 337-364): Springer Berlin / Heidelberg.

Zheng, D., Liu, Y., Zhao, J., and Saddik, A. E. (2007). A survey of RST invariant image watermarking algorithms. *ACM Comput. Surv.* 39(2), 5.

Zhou, F., Goel, M., Desnoyers, P., and Sundaram, R. (2011). Scheduler vulnerabilities and attacks in cloud computing. *Arxiv preprint arXiv:1103.0759*.

Zhu, C., and Hu, Y. (2008). A multipurpose watermarking scheme for image authentication and copyright protection. *Electronic Commerce and Security, 2008 International Symposium on*. 930-933.

Zhu, J., Wei, Q., Xiao, J., and Wang, Y. (2009). A fragile software watermarking algorithm for content authentication. *2009 IEEE Youth Conference on Information, Computing and Telecommunication, YC-ICT2009, September 20, 2009 - September 21, 2009*. Beijing, China: 391-394.