.

ENHANCING THE SECURITY OF HIGH PAYLOAD IMAGE

STEGANOGRAPHY USING CHAOS

REZZA MOIENI

A project report submitted in fulfillment of the

requirements for the award of the degree of

Master of Computer Science(Information Security)

Faculty of Computer Science and Information Systems

Universiti Teknologi Malaysia

JANUARY 2013

I dedicated this thesis to my beloved "Leyla" and my sweet daughter

For their endless support and encouragement

ACKNOWLEDGEMENT

IN THE NAME OF ALLAH, MOST GRACIOUS, MOST COMPASSIONATE

I would like to acknowledge my supervisor, Assoc. Prof. Dr. Subariah Ibrahim, for her support, encouragement, guidance, astute and expert editing. I would like to express gratitude for her patience, generosity and collaboration.

My amiable wife, sweet daughter; thank you for your perpetual encouragement and support. Your unwavering love that have shaped my mind and opened the doors of opportunity leading me to become the person I am today. Also I extend my thanks to my mother, father, brother and sister for their continuous charming support.

I would like to thank all of the individuals who have helped me during my thesis study.

ABSTRACT

One of the biggest technological events of the last two decades is the use of digital media in every aspect of daily life. Digital data can be stored efficiently in a very high quality format, and it can be manipulated very easily using computers. Digital image is one of the most popular digital multimedia data types. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. One of main concerns of these transmissions is security. To overcome this concern and security issues, steganography is one of main techniques that can provide confidentiality. Many steganography algorithms have been proposed. Each of them has its own drawbacks and advantages as well. LSB based technique in spatial domain is one of steganography techniques. Encryption can be simultaneously applied with steganography to increase the confidentiality of data. Among various techniques, chaos based encryption has attracted a lot of research and study due to good characteristics of the chaos systems. Yet, in order to transmit an image in a reasonable amount of time, some techniques must be incorporated to reduce the image's file size. Jpeg2000 is a well-developed image compression technique that can be utilized for this purpose. The common problem of image steganography is the need for imperceptibility for large amount of data. To overcome this problem, this project proposed a technique, S-UCLA (Steganography Using Compression and Lorenz Algorithms). S-UCLA combines KAMLA steganography technique with Lorenz chaotic map encryption and Jpeg2000 compression. The results show better imperceptibility can be obtained in comparison to KAMLA algorithm as PSNR and entropy has improved. Also the histogram for S-UCLA is smoother than KAMLA which showed better confusion and thus can be considered as providing higher confidentiality.

ABSTRAK

Salah satu peristiwa terbesar teknologi dua dekad yang lalu adalah penggunaan media digital dalam setiap aspek kehidupan seharian. Data digital boleh disimpan dengan cekap dan dengan kualiti yang sangat tinggi, dan ia boleh dimanipulasi dengan mudah dengan menggunakan komputer. Tambahan pula, data digital boleh dihantar dalam cara yang cepat dan murah melalui rangkaian komunikasi data tanpa kehilangan kualiti. Salah satu daripada kebimbangan utama transmisi ini adalah keselamatan. Untuk mengatasi kebimbangan ini dan isu-isu keselamatan, steganografi merupakan salah satu teknik utama yang boleh menyediakan kerahsiaan yang baik. Banyak algoritma steganografi telah dicadangkan. Teknik LSB berasaskan dalam domain ruang adalah salah satu teknik steganografi utama. Antara pelbagai teknik, penyulitan huru-hara berasaskan telah menarik banyak penyelidikan dan kajian kerana ciri-ciri yang baik sistem huru-hara. Namun, untuk menghantar imej dalam jumlah masa yang munasabah, teknik mesti diperbadankan untuk mengurangkan saiz fail imej. Masalah biasa steganografi imej adalah keperluan untuk imperceptibility untuk jumlah data yang besar. Untuk mengatasi masalah ini, beberapa algoritma dan teknik telah dibangunkan setakat ini. Dalam projek ini, algoritma steganografi KAMLA dengan pemetaan Lorenz huru-hara dan Jpeg2000 pemampatan adalah dicadangkan yang diberi nama S-UCLA. Hasil penelitian menunjukkan imperceptibility lebih lanjut dapat diperoleh dibandingkan dengan algoritma KAMLA sebagai PSNR dan entropi telah membaik. Juga histogram untuk S-UCLA lebih licin dari KAMLA. Kerahasiaan karena itu lebih dicapai.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1   Introduction

Nowadays, data is the most precious assets of the organizations and the value of each company is measured by the value of its information.   Information technology and data security in contrast, has become a very importantissue in recent years.Having a meaningful information security is the key for a successful competitive company.   Nowadaysintegrity, confidentiality and availability of the data which is being processed areone of the top concerns of companies which purchase technology products or implement services.   Information security means protecting precious information and systems related to that from unauthorized use, access, disclosure, disruption, changing and modification, perusal, recording or destruction.   The terms computer security, informationassurance and information security share the common goals of protecting the availability, integrity and confidentiality of information.   However, there are some subtle differences between them.

To meet the main characteristics of security, there are many specific security mechanisms includingciphering, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization, etc. Information hiding is among most important security mechanisms.

When communication via an un-trusted medium like the internet, it is important to protect information. Cryptography plays an important role in this field. Nowadays, cryptography uses principles from several disciplines such as computer science or mathematics. Steganography is composing hidden message or messages which only and only the sender of message and the receiver of message know the existence of that particular message. Nobody except these parties knows even the existence of the message. It even does not attract unwanted and superfluous attention. Steganography was used even in ancient times and these ancient methods are called physical steganography

At present, the way that information hiddenin image is based on spatial domain (Chang *etal.,* 2002) (Zhang *et al.,*2006) which mainly includes least significant bit (LSB) steganography and transformation domain (Cox *et al.,*1998).Due to high capability of hidden information and ease of implementation,spatial methods are the frequently used steganography technique. The main feature of information hiding algorithm based on spatial domain is that there is a relatively large amount of secret data, algorithm that is simple and easy to implement on the computer, and the disadvantage is lack of robustness, while information hiding algorithm based on transformation domain is that the embedded information energy is welldistributed, good robustness and high efficiency, but compared to spatial domain algorithm, amount of the embedded information is smaller and the algorithm is more complex.

Recently, techniques of hiding information have become important in many application areas. Lots of multimedia contents including digital audio, digital video, and digital pictures are increasingly utilized with distinguishing but hidden marks such as copyright notice or serial number. Military communication systems use traffic security technique increasingly which seek to conceal its sender, its receiver or even its existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections as well. Some steganography techniques are using simple algorithms such as least significant bit (LSB) insertion and noise manipulation, and transform domain and also image transformation like wavelet

transformation and discrete cosine transformation (DCT). Meanwhile, the quality and performance of image hiding is directly, related to capacity of hidden data. Using compression algorithms can decrease the size of hidden image without visually degrade the quality of hidden data before inserting it into cover medium. Meanwhile, using compression may increase the integrity of the steganography as compressed data are more resistant against degradations like noise.

JPEG2000 as a coding system and compression standard for images was introduced and developed by the committee of Joint Photographic Experts Group (JPEG). It was introduced in year 2000 with the goal of superseding their original discrete cosine transform-based popular JPEG standard with a newly designed, wavelet-based method. Meanwhile, the secrecy of steganography can be threatened if attacker knows the steganography algorithm. Since the steganography algorithms do no provide strong encryption, it is recommended to encrypt data before hiding it. Using steganography and cryptography together is a common practice.

Chaotic encryption technology has been applied vastly in the field of information encryption. Chaotic sequences have properties of determinacy, pseudo-randomness, periodicity and non-convergence, and they are sensitive dependence with the initial value.Therefore, chaotic sequence has good cryptography characteristics. According to the characteristics of chaotic sequence and information hiding based on spatial domain, a double algorithm is proposed based on LSB and Lorenz chaotic map taking image messages transmission as an example, and achieved information hiding. This algorithm is named Steganography Using Compression and Lorenz Algorithms (S-UCLA)

1.2   Background and Motivation

Increasing the power of computing systems has made the vulnerabilities to cryptographic methods as they can be broken more easily than before. So using

Steganography sometimes is a better choice as steganography avoid drawing suspicion to the existence of a hidden message as well as conceals content and location of data.

Digital image is one of the most popular digital multimedia data types. So, hiding information in a host image has attracted a lot of interest. It can be done without degrading the visual quality of the image. Lots of human eye characteristics and image parameters can gather together to perform acceptable results. Different sensitivity levels of human eye for construction of edges are used to obtain best results.

Hiding data in another data has long been a challenge. Today though we have one more challenge; how to hide a large amount of data in another one. Bitrate usually refers to the amount of data sent in a second and is usually measured as bit per second. However in steganography it refers to the amount of data that is hidden in a cover media. Information hiding in image can be categorized as high bitrate and low bitrate image hiding. An application of low bitrate image hiding is watermarking whereby small size data is embedded specially in order to verify the ownership in copyright applications. On the other hand, some applications need to hide relatively large amount of data within host image content. The main design goal of such system is to hide the secret message in an unnoticeable form. Although it may increase the storage size needed. Secure communication is the main application of high bitrate image hiding. There are four main categories of measuring the performance of high bitrate image hiding: (Nemati *et al.,* 2008)

- Transparency
- Channel capacity
- The impact of embedded information on the performance of image compression
- Robustness against lossy compression and noise

Lou *etal.*(2004) proposed a steganography scheme for secure communications based on thechaos which was using the randomness of chaos to make it more secure. In recent years, steganography techniques based on LSB methods, statistical properties, fractals and spread spectrum have been proposed. Liu *etal.*(2007) proposed an image steganography technique which is based on chaos mapping sequences in the spatial domain. Satisha*etal.*(2010) proposed spatial domain steganography using 1-Bit Most Significant Bit (MSB) with chaotic manner. In this technique cover image is separated into equal sized blocks of 8 by 8 matrix. But the block based image hiding is vulnerable to brute force attack. Song *etal.*(2011)proposed an information hiding method based on LSB and Tent chaotic map.First the secret message is encrypted using Tent chaotic map, and then LSB steganography is executed for the encrypted message in the cover-image. Compared to the traditional image information hiding method, the simulation results indicate that the method greatly improved in imperceptibility and security, and acquired good results.

1.3   Problem Statement

Limitation of secret image size threatens the secrecy of current image steganography techniques. An algorithm to overcome this problemis by combining Least Significant Bit technique with Lorenz Chaotic map encryption and Jpeg-2000 Compression method is proposed.

1.4   Research Goal

The main aim of this project is to overcome the problems of hiding image in image where the secret image or images are as large as the cover one and to increase the confidentiality of LSB based algorithm. The proposed algorithm is combining Jpeg2000 Compression algorithm with LSB and Lorenz chaotic mapping.

1.5   Research Objectives

To fulfill the research goals, the following objectives are specified:

(i)   To study the techniques of hiding images in another image

(ii)   To enhance an LSB based steganography algorithm that hide high capacity data inside a color image to increase confidentiality

(iii)   To analyze the performance of the proposed algorithm

1.6   Research Scopes

The scope of the project is as follows:

(i) Colored still image information in spatial domain. Cover image is uncompressed 512 by 512 TIFF color image and Secret image is 256 by 256 TIFF color image.

(ii) Implementation with MATLAB

(iii) The evaluated metrics are Histogram, Entropy and PSNR

1.7   Significance of the Research

Advantages of transmission data in digital formats via networks are not negligible in terms of cost, ease of use, speed, facilities and flexibility. All these points are meaningful since the security basics of our data and transmission including confidentiality, integrity and availability are satisfied. Importance of these is more highlighted in multimedia usage as they carry high bitrate data that is on a growing path nowadays. There are few reliable tools for this area in military, telemedicine, Video-on-demand, Broadcast usage, etc.

REFERENCES:

Ahmidi.N.& LotfiNeyestanak. (2008). A human visual model for steganography. *Canadian Conference on Electrical and Computer Engineering*, 001077-001080.

Ale.Z. (2011). A Hash-Based Approach for Color Image Steganography,303-307.

Ali. M., Younes.B & Jantan.A. (2008). A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion,*8*(6), 2-9.

Amin.M, Salleh.M & Ibrahim.S.(2003) "Information Hiding Using Steganography",*4th National Conference On Telecommunication Technology Proceedings (NCTT2003)*, Shah Alam, Malaysia, pp. 21-25, January 14-15.

Artz. C, (2001) " Digital Steganography: Hiding Data within Data", *IEEE Internet Computing*, pp. 75-80.

Bailey.K, Curran.K. (2006). An evaluation of Image Based Steganography methods.*Multimedia Tools and Applications* (Vol. 30, pp. 55-88).

Buck. I. & Kozyrakis. S. C. (2007). GPU Computing: Programming a Massively Parallel Processor, 7695.

Chan, Kwong.C, Cheng.L.M., Leung, K.chi, Li &S.ling, (2004) . Image Hiding Based on Block Difference. *Technology, I., & Kong, H.*, 968-972.

Chan, C.K., & Cheng.L.M. (2004). Hiding Data in Images by Simple LSB Substitution.*Pattern Recognition*, *37*(3), 469-474.

Chan & Kuan.M.(2001). Concealing a Secret Image Using the Breadth First Traversal Linear Quadtree Structure. *Proceedings of the Third International Symposium on Cooperative Database Systems for Advanced Applications. CODAS 2001*, 194-199. IEEE Comput. Soc.

Cachin.C, (1998) "An Information-Theoretic Model for Steganography", *in proceeding 2nd Information Hiding Workshop,* vol.1525, pp.306-318.

Chandramouli.R., & Subbalakshmi.K. (2004). Current TrendsIn Steganalysis : A Critical Survey.*Stevens Institute of Technology,* (December), 964-967.

Chandramouli.R & N.Memon, (2001) "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022.

Chang C, Chen, Lin & Chang.L,.(2003). Scheme for Sharing a Secret Color Image.

Chang, C. -., Chen, G. -., & Lin, M. -. (2004). Information hiding based on search-order coding for VQ indices. *Pattern Recognition Letters, 25*(11), 1253-1261.

Chang, C.C., & Tseng, H.-W.(2009). Data Hiding in Images by Hybrid LSB Substitution.*2009 Third International Conference on Multimedia and Ubiquitous Engineering*, 360-363.

Che.S., Huang Q., & Ma.B. (2008). Adaptive Image Hiding Algorithm Based on Classification.*2008 Eighth International Conference on Intelligent Systems Design and Applications*, 314-319.

Cheddad.A., Condell.J., Curran.K., & McKevitt.P. (2008). Securing information content using new encryption method and Steganography.*2008 Third International Conference on Digital Information Management*, (1), 563-568.

Chen.S, (2011). A Module-Based LSB Substitution Method with Lossless Secret Data Compression.*Computer Standards & Interfaces*, *33*(4), 367-371. Elsevier B.V.

Chen, S.-K., & Wang, R.-Z.(2010). High-Payload Image Hiding Scheme Using k-Way Block Matching.*2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 70-73.

Chung KL. & Chang LC. (1998). Large encryption binary images with higher security. Pattern Recognition Letter;19(56):461–8.

Cvejic.N. & Seppanen.T. (2004). Channel Capacity of High Bit Rate Audio Data Hiding Algorithms in Diverse Transform Domains.*In Proceedings of the international symposium on communications and information technologies* (ISCIT 2004)

Coe, J. I. M. (2010). Steganography by hiding data in tcp/ip headers 4, 61-65.

Christian Rey&Jean-Luc Dugelay (2002), "A Survey of Watermarking Algorithms for Image Authentication", EURASIP Journal on Applied Signal Processing Volume 2002 , Issue 6, Pages 613-621

Lorenz& Edward Norton (1963)."Deterministic Non-Periodic Flow".*Journal of the Atmospheric Sciences* **20** (2): 130–141.

El-emam.N.. (2008).Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm, 95-106.

Enayatifar.R.; Mahmoudi.F.&Mirzaei.K.(2009) , "Using the Chaotic Map in Image Steganography," *Information Management and Engineering, 2009. ICIME '09. International Conference*, vol., no., pp.491-495, 3-5 .

Ge.H., Huang.M., & Wang.Q. (2011). Steganography and steganalysis based on digital image. *2011 4th International Congress on Image and Signal Processing*, 252-255.

Gupta.S., & Biswas.R. (2012). A Performance Evaluationof JPEG Steganography, 1-9.

Gunsel.B., Uludag.U., & Tekalp.A.M (2002). Robust Watermarking of Fingerprint Images. *Journal of pattern recognition*, 35(12), 2739-2747

Hamid.R Nemati & Yang.L (2011), Applied Cryptography for Cyber Security and Defense.. New York: Hershly, 244~254.

Hmood.A.K., H.A. Jalab.Z.M. Kasirun, Zaidan.B.B & Zaidan.A.A, (2010). On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Jastrzebski.K & Kotulski.Z. (2009), An Improved Image Encryption Scheme Based on Chaotic Map Lattices.Eng Trans 2009; 57(2):69–84.

Jiang.H, Yan, & Fu.C.(2008). An Image Encryption Scheme Based on Lorenz Chaos System.*2008 Fourth International Conference on Natural Computation*, 600-604.

J.Fridrich and M.Goljan, (2003) Digital image steganography using stochastic modulation," *SPIE Symposium on Electronic Imaging, San Jose, CA,*.

K., M. S., & Yaghoobi, M. (2008).A Simple and Robust Approach for Image Hiding Using Chaotic Logistic Map.*2008 International Conference on Advanced Computer Theory and Engineering*, 623-627.

Kanso.A., & Ghebleh.M. (2012). A Novel Image Encryption Algorithm Based on a 3D Chaotic Map. *Communications in Nonlinear Science and Numerical Simulation*, *17*(7), 2943-2959. Elsevier B.V.

Kekre.H. B., Athawale.A., Halarnkar.P. N., & Stage.A. E. (2008). Increased Capacity of Information Hiding in LSB ' s Method for Text and Image, 246–249.

Kekre.H. B., & Athawale, A. A. (2011). Increased Cover Capacity using Advanced Multiple LSB Algorithms, (Icwet), 25–31.

Kim.K.-J., JungK.H., & Yoo.K.Y.(2008). A High Capacity Data Hiding Method Using PVD and LSB.*2008 International Conference on Computer Science and Software Engineering*, (1), 876-879.

Kumar.A., & Pooja.K. (2010).Steganography- A Data Hiding Technique.*International Journal of Computer Applications*, *9*(7), 19-23.

Lee.C.F., Shen.J..J., & Chuang.M.C.(2009). An Embedding Technique Based upon Block Prediction and Code Cascading Shift.*2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 361-364.

Lee.C.,Wang, Ren.Y, Chang.C. & Chung.N. (2007).A Steganographic Method with High Embedding Capacity by Improving Exploiting Modification Direction, 3-6.

Lee, Y.-P., Lee, J.-C., Chen, W.-K., Chang, K.-C., Su, I.-J., & Chang, C.-P.(2012). High-payload Image Hiding with Quality Recovery Using Tri-way Pixel-Value Differencing.*Information Sciences*, *191*, 214-225. Elsevier Inc.

Li.X., Qi.Z., Yang, Z., & Kong, J. (2009). A Novel Hidden Transmission of Biometric Images Based on Chaos and Image Content. *2009 First International Workshop on Education Technology and Computer Science*, 21-25.

Li.Y., & Zhang.Q. (2010). A stratified image-hiding method based on chaos. *2010 IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA)*, (l), 1-5.

Lin, S. D. (2004). A Suitable Image Hiding Scheme for JPEGImages.*2004 International Conference on Image Processing, 2004. ICIP '04.*, *3*, 1565-1568.

Liu.C., Ouyang.C., Guo.M., & Chen.H. (2010). Image Steganalysis Based on Spatial Domain and DWT Domain Features. *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, 329-331.

Liu.N., & Guo.D. (2007).Multiple Image Information Hiding Technique Based on Chaotic Sequences.*2007 International Conference on Convergence Information Technology (ICCIT 2007)*, 1720-1725.

Lou.D.-C., & Sung, C.-H.(2004). A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem.*IEEE Transactions on Multimedia*, *6*(3), 501-509.

Luo.W., Huang.F., & Huang.J. (2010). Edge Adaptive Image Steganography Based on LSB Matching Revisited. *IEEE Transactions on Information Forensics and Security*, *5*(2), 201-214.

Matthews.R. (1989). On the Derivation of AChaotic Encryption Algorithm[J]. Cryptologia ,8 (1):29-42

Mathkour.H., Al-Sadoon.B., & Touir.A. (2008). A New Image Steganography Technique.*2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 1-4.

Medeni.O., & Mamoun.E. (2010). A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution, 1-4.

Menezes A, Van Oorschot P, Vanstone S. Handbook of Applied Cryptography.Boca. Raton, FL: CRC Press; 1997

Networks.C., Tech.J. K. M., & Oberoi.A. (2012).Image Steganography by Using Mapping of Letters to Pixels and indicator, *2*, 186-188.

N.F.Johnson& S.Jajodia,(1998) "Steganalysis of Images Created Using Current Steganography Software", *in Proceeding for the Second Information Hiding Workshop, Portland Oregon*, USA, pp. 273-289.

N.F.Johnson and S.Jajodia,(1998) "Exploring Steganography: Seeing the Unseen", IEEE, pp. 26-34.

Pavlidis.G., Tsompanopoulos.A., Papamarkos.N., & Chamzas.C. (2002). JPEGZOOO Over Noisy Communication Channelsthe Cost Analysis Aspects, 5–8.

Provos.N.P. Honeyman, (2001) " Detecting Steganography Content on the Internet" *.CITI Technical Report 01-11*.

Petitcolas.F.A.P., Anderson.R.J., & Kuhn.M.G. (1999). Information Hiding — A Survey, *87*(July), 1062-1078.

R A Isbell,(2002) "Steganography: Hidden Menace or Hidden Savior", *Steganography White Paper*, 10 May 2002.

Raphael.A.J. (2011). Cryptography and Steganography – A Survey, *2*(3), 626-630.

R.J.Anderson, F.A.P.(1998). Petitcolas, "On the Limits of Steganography", *IEEE Journal of Selected Area in Communications, pp.474-481*.

S.Tanako, K. Tanaka & T.Sugimura,(2000) "Data Hiding via Steganographic Image Transformation", IEICE Trans. Fundamentals, vol.E83-A, pp. 311-319.

Sakyte.E., Palivonaite, R., Aleksa, A., &Ragulskis, M. (2011). Image Hiding Based on Near-Optimal Moiré Gratings. *Optics Communications*, *284*(16-17), 3954-3964. Elsevier B.V.

Saltzman, Barry (1962). "Finite Amplitude Free Convection as an Initial Value Problem—I".*Journal of the Atmospheric Sciences* 19(4): 329–341.

Sathisha.N., Madhusudan, G. N., Bharathesh, S., Suresh Babu, K., Raja, K. B., &Venugopal, K. R. (2010). Chaos based Spatial Domain Steganography using MSB. *2010 5th International Conference on Industrial and Information Systems*, 177-182.

Satish.K., Jayakar.T., Tobin.C., Madhavi, K., &Murali, K. (2004). Chaos based spread spectrum image steganography. *IEEE Transactions on Consumer Electronics*, *50*(2), 587-590.

Shi.P. (2010). A technique of improved steganography text based on chaos and BPCS. *2010 2nd International Conference on Advanced Computer Control*, 232-236.

Singh.K. M., Singh, S .B., &Singh, S. S (2007). Hiding encrypted message in the features of images. *International journal of computer science and network security (IJCSNS), 7(4)*

Song.J., & Ding, Q. (2011). An Information Hiding Method Based on LSB and Tent Chaotic Map, *8009*(Icdip), 800920-800920-4.

S.S. Maniccam & N. G. Bourbakis,(2004) "Image and video encryption using SCAN patterns", Pattern Recognition, 2004, vol. 37, pp. 725–737

Suleiman, M., &Rababaa, A. (2009).Colored Image-In-Image Hiding, 24-28.

Sur, A., Goel, P., &Mukhopadhyay, J. (2008).A Spatial Domain Steganographic Scheme for Reducing Embedding Noise, (March), 12-14.

Wang.R.-Z., Lin.C.-F., & Lin, J.-C.(2001). Image hiding by optimal LSB substitution and genetic algorithm.*Pattern Recognition*, *34*(3), 671-683.

Wu.D. C., & Tsai, W.H. (2000). Spatial-domain image hiding using image differencing.*IEE Proceedings - Vision, Image, and Signal Processing*, *147*(1), 29.

Wu, D.-C., & Tsai, W.-H.(2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, *24*(9-10), 1613-1626.

Yan, W., & Ping, L.-di. (2009). A New Steganography Algorithm Based on Spatial Domain. *2009 Second International Symposium on Information Science and Engineering*, 171-176.

Yang.C.Y., Huang.W.Y., & Cheng.Y.F.(2007). Image Hiding by Simple Module Substitution. *Second International Conference on Innovative Computing, Information and Control (ICICIC 2007)*, 289-289.

Yang.C.-T., Huang.C.L., Lin.C.-F., & Chang, T.-C. (2010). Hybrid Parallel Programming on GPU Clusters. *International Symposium on Parallel and Distributed Processing with Applications*, 142–147.

Yu.L., Zhao, Y., Ni.R., & Li.T. (2010).Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm.*EURASIP Journal on Advances in Signal Processing*, *2010*(1), 876946.

Zhang.W., Cheung.S., & Chen, M. (2005).Hiding privacy information in video surveillance system. In proceedings of the international conference on image proceeding (ICIP'2005), 3, II-868-71

Zhao.Y., Zhao.N., Ren, G., & Zhang, B. (2006).A Novel Large Capacity Image Hiding Method Based on the Orthogonal Chaotic Sequences.*2006 International Conference on Intelligent Information Hiding and Multimedia*, 613-616.

Zhou.C.-S., Niu.L.-H., & Liu, J. (2010). Research on Component and DAG Based Dynamic Workflow System. *2010 First International Conference on Pervasive Computing, Signal Processing and Applications*, 1228-1231.