American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-11, pp-122-128
www.ajer.org

Research Paper Open Access

Steganography: A Review of Information Security Research and Development in Muslim World

Yunura Azura Yunus, Salwa Ab Rahman, Jamaludin Ibrahim
Kuliyyah of Information and Communication Technology International Islamic University Malaysia
Kuliyyah of Information and Communication Technology International Islamic University Malaysia
Kuliyyah of Information and Communication Technology International Islamic University Malaysia

Abstract: - Conveying secret information and establishing hidden relationship has been a great interest since long time ago. Therefore, there are a lot of methods that have been widely used since long past. This paper reviewed one of the methods for establishing hidden communication in information security and has gained attraction in recent years that is Steganography. Steganography is the art and science of hiding a secret message in a cover media such as image, text, signals or sound in such a way that no one, except the intended recipient knows the existence of the data. In this paper, the research and development of steganography from three years back starting from 2010 until recently, 2013 in Muslim world are reviewed. The future research in the field of Steganography is briefly discussed.

Keywords: - *Cover Image, Stego Image, Cryptography, Steganography, Information Hiding, Information Security, Muslim World*

a. INTRODUCTION

In today's information technology era, the internet has played a vital part in the communication and information sharing. Due to the rapid development in Information Technology and Communication and the Internet, the security of the data and the information has raise concerned. Every day, confidential data has been compromised and unauthorized access of data has crossed the limits. Great measures should be taken to protect the data and information [1,2]. Steganography combined with encryption will be a powerful and efficient tool that provides high level of security [3].

A review on steganography research and development throughout the year will be discussed in part 2 of this paper. The review will be focusing on Muslim world and narrowing it down to Middle East countries. The review includes past, current and future research on steganography and the possible future research on the latest algorithm and technologies in steganography.

II. MUSLIM WORLD TERMINOLOGIES

The term Muslim World is also known as the Ummah and Islamosphere [4]. There are different meanings referring to the term. In a religious sense, the Islamic Ummah is referring to those who follow the teachings of Islam referring to as a Muslim. In a cultural sense, the Muslim Ummah is referring to the Islamic civilization, this inclusive of non-Muslims living in the civilization. In a modern geopolitical sense, the term Muslim World is referring to collectively to Muslim-majority countries. As of 2010, over 1.6 billion or about or about 23.4% of the world population is Muslims [5]. 62% of Muslims live in Asia-Pacific [6], 20% in the Middle East-North Africa [7], 15% in Sub-Saharan African [8], around 3% in Europe [9] and only 0.3% in the Americas [10][11][12][13]. This paper focuses on steganography research and development in Muslim World narrowing it down to Middle East countries. The majority of the population in Middle East countries are Muslim [14].

III. STEGANOGRAPHY HISTORY

The word Steganography comes from the Greek origin that means "concealed (covered) writing". The word 'steganos' means "covered or protected" and 'graphie' means "writing" [15]. Steganography thus not only emphasize on the art of hiding information but also the art and science of hiding the communication that take place [16]. First applications of Steganography were documented by Herodotus, a Greek historian. Steganography can be traced back to ancient Greek centuries when the message is tattooed on the messengers shaved heads. The hair then grows to hide the message. Their head will be shaved when they reach the recipient of the message [17,18,19].Another steganography method that was used during those days is tablet wax. In order to hide the message, the tablet was erased by wax and text was etched on and then again covered it by wax and appeared blank upon inspections [18,20].

During the century, the methods of using invisible inks were extremely popular [18]. During the World War II where people used ink for writing hidden messages, this was true [17]. The mixture will turn darker and the written message becomes visible upon heating. After some time, the Germans introduced the microdot technique where microdots are considered as photographs as small as a printed period, but with a clear format of a typewritten page [17, 21]. They were included in a letter or an envelope, and because of their tiny sizes, they could be indiscernible. Microdots were also hidden in body parts including nostrils, ears, or under fingernails [18].The military and several governmental agencies are looking into steganography for their own secrettransmissions of information. They are also desirous of discerning secret information communicated by criminals, terrorists, and other aggressive forces. Following investigations into the Al-Qaeda attack, steganography was suspected to be made use of in their attack of the World Trade Centre [22].

3.1 STEGANOGRAPHY FEATURES AND APPLICATIONS

Steganography can be used in a lot of useful applications. For example copyright control of materials, to enhance the robustness of an image search engines and smart identity cards where the details of individuals are embedded in their photographs. Other applications include video-audio synchronization, TV broadcasting, TCP/IP packets where a unique ID is embedded in an image to analyse the network traffic of particular users [20]. Medical Imaging Systems is one of the modern applications that use Steganography where a separation is recommended between patients' image data or DNA sequences and their captions for security or confidentiality reasons. Thus, embedding the patient's information in the image could be a security measure to help solving security issues [23].Digital technologies have swept the confidence in the integrity of visual imagery [24]; a matter that motivated researchers to conduct research on digital document forensics. In 2009, Cheddad and his colleagues propose a steganographic scheme which protects scanned documents from forgery using self-embedding techniques. It also allows legal or forensics experts to access the original document though it is manipulated [25].

3.2 THE DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY

Users on the internet have to send, share or receive confidential data most of the time [26]. With the increasing number of users and the increasing number of unauthorized access of confidential data, information security played an important role. Therefore, the main issue now is to mitigate and to lessen the impact of the chances of the information being detected during transmission. Cryptography deals message encryption but the communication is easily aroused suspicious but on the other hand, steganography deals with secret message hiding but the communication is invisible. This is the major differences between cryptography and steganography.

It is often thought that by encrypting the traffic, the communications will be secured but this has not been adequate in real live situation [27]. In cryptography method, people become aware of the existence of information by observing coded information, although they are unable to comprehend the information. Steganography hides the existence of the message so that intruders can't detect the communication and thus provides a higher level of security than cryptography. Both steganographic and cryptographic systems provide secret communications but different in terms of system breaking. If the intruder can read the message in cryptographic then it is broken but steganographic is considered broken once the intruders detect the existence of the secret message [28]. Steganography system is more fragile than cryptography systems in terms of system failure. This is because if the communication is detected even without decoding the message, a steganographic system is considered a failure [29].

3.3 A REVIEW OF STEGANOGRAPHY RESEARCH AND DEVELOPMENT IN MUSLIM WORLD

Table 1 : A review of steganography research and development

No	Title	Year	Country	Keyword	Summary
1.	A modified high capacity image steganography technique based on wavelet transform [30]	2010	Iraq and United Kingdom	Steganography, security, wavelets, cryptography, and information hiding	This paper proposed a modified high-capacity image steganography technique that uses wavelet transform. The wavelet transform must be at acceptable levels of imperceptibility and distortion in the cover image.
2.	Arabic/Persian text steganography utilizing similar letters with different codes [31]	2010	Iran	information hiding, Persian/Arabic text, text steganography, Unicode	This paper proposeda new method in hiding information by using Persian (Farsi) and Arabic texts. In the Unicode Standard, "Ya" and "Kaf" are two different characters having the same shape. The two characters used different codes at the beginning or in the middle of the words. Thus, the information can be hidden in texts using one of these two characters. The method has been used by Java Programming Language.
3.	Using contourlet transform and cover selection For secure steganography [32]	2010	Iran	Contourlet transform, Steganography,Steganalysis,Cover selection, Image complexity	This paper proposed a new adaptive contourlet-based steganography method. The method decomposes the cover image by contourlet transform. The authors also investigate the effect of cover selection on steganography embedding and steganalysis results.
4.	An arabic text steganography technique using zwj and zwnj regular expressions [33]	2011	Jordan	Arabic text, Unicode, cryptography, hiding information, text steganography	This paper proposed a text steganography technique for Arabic Unicode texts. Arabic Unicode text uses two special characters that arethe zero width joiner character (JWZ) to join two letters and the zero width non joiner character (JWNZ) to prevent two letters from joining. The authors use two regular expressions to generate a sequence of special characters that consists of JWZ and JWNZ characters for information hiding.
5.	Steganography In Programming [34]	2011	Iran	Steganography, Trithemius, Methods, Microdot	This paper reviewed different steganography methods that are text, photo or sound. There are three methods studied in text steganography that are life shift coding, word shift coding and feature coding. In photo steganography the authors observed filtering and masking methods. While in sound steganography, the methods are bit insertion, phase coding, spread spectrum coding and echo hiding. Steganalysis or the science of finding hidden information is also discussed.
6.	Blind Colour Image Steganography in Spatial Domain [35]	2011	Iraq	information hiding, colour image steganography, spread spectrum	This paper proposed a blind colour image steganography method that embeds secret message by spraying theme on the blocks in the high order bits in colour channel such as blue. However it also depends on the constant sequence spread spectrum method to survive loss compression image like JPG.

7.	Microdots DNA Steganography [36]	2011	Iraq	Steganography, DNA, DNA computing. Microdots, DNA steganography	This paper reviewed the use of DNA computing in steganography and the fundamentals of DNA. DNA computing in steganography has been recognized as a future technology that can help in unbreakable algorithms. The authors then proposed new ideas to enhance the established method.
8.	Steganography in Digital Images: Common Approaches and Tools [37]	2013	Saudi Arabia and Malaysia	Digital image steganography, Frequency domain, Spatial domain, Steganalysis.	This paper presents common approaches and tools that are used in digital image steganography. It is shown mathematically and graphically. The differences between steganography, cryptography and watermarking technique are discussed. The authors also highlighted the current steganography tools and demonstrate how the secret information is embedded into image through the tools.
9.	Optimal Image Steganography Content Destruction Techniques [38]	2013	Iraq	Steganography, stego-destruction, DCT, LSB, Denoising and Filtering, overwriting	The paper presents two methods for destroying steganography content in an image that are the overwriting and the denoising method. The overwriting method is a random data that can be written again over steganographic images while the denoising method uses two kinds of destruction techniques that are filtering and discrete wavelet techniques.These two methods have been simulated and evaluated over two types of hiding techniques that are Least Significant Bit LSB technique and Discrete CosineTransform DCT technique.
10.	Steganography in image files: A survey [39]	2013	Iraq and Malaysia	Image files, Spatial Domain, Steganography, Survey, Taxonomy, Transform Domain	This paper presents the use of an image file as a carrier and the taxonomy of current steganographic techniques. The authors analysed and discussed steganography techniques for their ability in information hiding and the robustness to different image processing attacks. They also briefly discussed steganalysis which is the science of attacking steganography.

Table 1: Illustrates a review of Steganography research and development in the Muslim world from the year 2010 until 2013. In 2010, there are three researches being reviewed.

3.3.1 The first research proposed a modified high capacity image steganography technique that uses wavelet transform. The second research proposed a new method in hiding information by using Persian (Farsi) and Arabic texts while the third research proposed a new adaptive contourlet-based steganography method. The similarities of all these three researches are they are proposing a new method or technique in the field of steganography. The first and the third research are focusing on image steganography while the second research is focusing on text steganography.

3.3.2 In 2011, there are four researches being reviewed. The first research proposed a text steganography technique for Arabic Unicode texts. Arabic Unicode text uses two special characters that are the zero width joiner character (JWZ) to join two letters and the zero width non joiner character (JWNZ) to prevent two letters from joining. Two regular expressions are used to generate a sequence of special characters that consists of JWZ and JWNZ characters for information hiding. The second research reviewed different steganography methods that are text, photo or sound. There are three methods studied in text steganography that are life shift coding, word shift coding and feature coding. In photo steganography, filtering and masking methods are observed. While in sound steganography, the methods are bit insertion, phase coding, spread spectrum coding and echo

hiding. The third research proposed a blind colour image steganography method that embeds secret message by spraying theme on the blocks in the high order bits in colour channel such as blue while the fourth research reviewed the use of DNA computing in steganography. The fundamentals of DNA are discussed and new ideas are proposed to enhance the established method.

3.3.3 In 2013, there are three researches being reviewed. The first research presents common approaches and tools that are used in digital image steganography. It is shown mathematically and graphically. The differences between steganography, cryptography and watermarking technique are discussedand the current steganography toolsused are also highlighted. The second research presents two methods for destroyingsteganography content in an image that are the overwriting and the denoising method. The overwriting method is a random data that can be written again over steganographic images while the denoising method uses two kinds of destruction techniques that are filtering and discrete wavelet techniques. While the third research presents the use of an image file as a carrier and the taxonomy of current steganographic techniques. Steganography techniques are analysed and discussed for their ability in information hiding and the robustness to different image processing attacks.

3.3.4 From the three consecutive years from 2010 to 2013, the image steganography is the most popular choice of researchers. There are four main categories that used in steganography that are image, audio, sound and protocol [1]. Out of the ten researches, five is proposing new techniques or methods in image steganography. Nearly all digital file formats can be used for steganography but the formats that are more compatible are those with high degree of redundancy. The terms redundancy means the bits of an object that provide accuracy far greater than necessary for the object's use and display [40]. The redundant bits of an object then can be altered without the alteration being detected easily [22]. Image files usually comply with this main requirement even though research has also uncovered other types of file formats that also can be used for hiding information.

IV. FUTURE RESEARCH

As steganography continue on its evolutionary path, the world of information security looks forward in the future research regarding the field of steganography as modern encryption algorithms are broken. Some of the future researches include:

1. Steganalysis that is defined as a process to crack the cover object in order to get the hidden information.
2. Combining the technology of cryptography with steganography to achieve a higher level of security that even the intruder detects the hidden message, the message cannot be decoded.
3. Researchers continue to discover new platforms that could potentially use to hide information apart from the traditional platforms such as audio, video and images.
4. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology for unbreakable algorithms.

V. CONCLUSION

As per conclusion, this paper discussed an overview of Steganography, the features and applications, history and how it's differs from cryptography. This paper also highlighted a review of research and development of Steganography in Muslim world from the year 2010 to 2013. This paper suggested a few for future research like Steganalysis, technology combined, discover new platform and possible unbreakable algorithms.

REFERENCES

[1] T. Morkel , J.H.P. Eloff and M.S. Olivier "An Overview of Image Steganography".
[2] Amanpreet Kaur, Renu Dhir, and Geeta Sikka "A New Image Steganography Based On First Component Alteration Technique" (IJCSIS) International Journal of Computer Science and Information Security,Vol. 6, No. 3, 2009.
[3] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al-Qershi "ImageSteganography Techniques: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (3): 2013.
[4] Amir Ahmad Nasr. My Isl@m: How Fundamentalism Stole My Mind --- and Doubt Freed My Soul. Page 147. 2013.
[5] "Executive Summary". The Future of the Global Muslim Population. Pew Research Center. 27 January 2011. Retrieved 1 November 2013.

[6] "Region: Asia-Pacific". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
[7] "Region: Middle East-North Africa". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
[8] "Region: Sub-Saharan Africa". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
[9] "Region: Europe". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
[10] "Region: Americas". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
[11] Tom Kington (31 March 2008). "Number of Muslims ahead of Catholics, says Vatican". The Guardian. Retrieved 1 November 2013.
[12] "Muslim Population". IslamicPopulation.com. Retrieved 1 November 2013.
[13] "Field Listing - Religions". Retrieved 1 November 2013.
[14] "Muslim Population by Country". The Future of the Global Muslim Population. Pew Research Center. Retrieved 1 November 2013.
[15] Rajkumar Yadav "Study of Information Hiding Techniques and their Counterattacks: A Review Article" , International Journal of Computer Science & Communication Networks, Vol 1(2), 142-164, Oct-Nov 2011.
[16] Angela D. Orebaugh " Steganalysis: A Steganography Intrusion Detection System" , George Mason University
[17] R. Krenn, "Steganography and steganalysis," An Article, Santa Barbara, California, January 2004, available from: http://www.krenn.nl/univ/cry/steg/article.pdf [Last accessed on 1 November 2013]
[18] J.C. Ingemar, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, "Digital watermarking and steganography", Burlington: Morgan Kaufmann; 2008.
[19] J. Fridrich, "Steganography in Digital Media: Principles",Algorithms, and Applications, Cambridge, England: Cambridge University Press; 2009.
[20] N.F. Johnson, and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, IEEE, Vol. 31, pp. 26-34, 1998.
[21] T. Morkel, J.H.P. Eloff, and M.S. Olivier, "An overview of image steganography" in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, pp. 1-12, 29 Jun.-1 Jul. 2005.
[22] M. Bachrach, and F.Y. Shih, "Image steganography and steganalysis,"Wiley Interdisciplinary Reviews: Computational Statistics, Vol. 3, pp. 251-9, 2011.
[23] Petitcolas, F.A.P." Introduction to information hiding". In S. Katzenbeisser & F. A. P. Petitcolas (Eds.), Information hiding techniques for steganography and digital watermarking (pp. 1-12). Boston, London: Artech House,2000.
[24] Farid, H. "Image forgery detection". Signal Processing Magazine, IEEE, 26(2): 16-25. doi: 10.1109/msp.2008.931079, 2009.
[25] Cheddad, A., J. Condell, K. Curran, & P. Mc Kevitt. "A skin tone detection algorithm for an adaptive approach to steganography". Signal Processing, 89(12): 2465-2478. doi: 10.1016/j.sigpro.2009.04.022, 2009.
[26] Arvind Kumar and Km. Pooja "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.
[27] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn "Information Hiding A Survey"Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.
[28] Banasthali Vidyapith, Rjasthan "Image Steganography Techniques: A Review Article", Bulletin of Engineering, Faculty of Engineering, Hunedoara, Romania, July-September,2013.
[29] Adel Almohammad "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility" A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing, Brunel University, August,2010.
[30] Ali Al-Ataby, Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform,"The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.
[31] M. Hassan Shirali-Shahreza, Mohammad Shirali-Shahreza, "Arabic/Persian Text Steganography Utilizing Similar Letters With Different Codes," The Arabian Journal for Science and Engineering, Volume 35, Number 1B, April 2010.

[32] Hedieh Sajedi, Mansour Jamzad, "Using contourlet transform and cover selection for secure steganography," Springer, Int. J. Inf. Secur. (2010) 9:337–352, August 2010.
[33] A.F. Al Azawi, M.A. Fadhil, "An Arabic Text SteganographyTechnique Using Zwj And Zwnj Regular Expressions," International Journal Of Academic Research Vol. 3. No. 3. May 2011.
[34] Mahmoud Vaziri Nasab , Behzad Mahjour Shafiei, "Steganography In Programming," Australian Journal of Basic and Applied S ciences, 5(12): 1496-1499, 2011.
[35] F. A. Abdullatif, W. A.Shukur," Blind Color Image Steganography in Spatial Domain," Ibn Al- Haitham J. For Pure & Appl. Sci. Vol.24 (1) 2011.
[36] Wissam Makki Alwash, "Microdots DNA Steganography," Journal of Babylon University/Pure and Applied Sciences/ No.(3)/ Vol.(19): 2011.
[37] Samer Atawneh, Ammar Almomani1 and Putra Sumari, "Steganography in Digital Images: Common Approaches and Tools,"IETE Technical Review, Vol 30, Issue 4, Jul-Aug 2013.
[38] Siddeeq Y. Ameen, Muthana R. Al-Badrany, "Optimal Image Steganography Content Destruction Techniques," Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics, 2013.
[39] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Dheiaa Najim, Lubna Kanaan, "Steganography in image files: A survey," Australian Journal of Basic and Applied Sciences, 7(1): 35-55, 2013.
[40] W Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, Vol. 35, No. 3 and 4, pp. 313-336,1996.
[41] Mehdi Kharrazi, Husrev T. Sencar and Nasir Memon "Image Steganography : Concepts and Practices "Polytechnic University, Brooklyn, NY 11201, USA.