International Journal of Engineering & Technology, 7 (2.14) (2018) 89-92

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Comparative Review on Feature-content Based of Public Key Steganography Trends

Nor Hafizah Abdul-Razak [1]*, Roshidi Din[2], Mazida Ahmad[2]

[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Malaysia
[2]School of Computing, College of Arts and Sciences, Universiti Utara Malaysia
**Email: norhafizahrazak@gmail.com*

Abstract

This paper intends to provide an up-to-date review on studies conducted in the field of Public Key Steganography (PKS). It is based on feature-content of PKS which are domain, scheme, and evaluation parameter aspects. It is concentrate on type of domain in PKS; schemes applied in PKS, and commonly used evaluation parameters in evaluating the performance of PKS system. Findings of this study are grouped into several subsections based on type of domain, schemes, and evaluation parameters. This review provides brief information related to important component in PKS environments. It provides an added value to the knowledge of PKS and also as a source of information to other researchers in conducting their study in the field of PKS. Besides, this study also provides a recommendation and good practices drawn from the reviewed literatures.

Keywords: *Domain Aspect; Evaluation Parameter Aspect; Review Criteria; Scheme Aspect*

1. Introduction

Digital communication has become an essential part of infrastructure nowadays, a lot of applications are Internet-based and in certain cases the communication is required to be made secret. To achieve this goal, one of the techniques used is steganography. Steganography is a mechanism used to embed hidden content in unremarkable cover object so as not to arouse an eavesdropper's suspicion [1]. Generic steganography model consist of three components; first is cover object which is the carrier used to carry hidden message. In steganography, type and method is differentiated on the basis of cover object used which is text, image, audio, or video [2]. Second is the hidden message which can be in any form such as text or image. Lastly, the key use to discover the hidden message. Two main stages involve in generic steganography model are embedding and extracting process. Embedding process is used to hide hidden message in the cover object by using stego key. As in extracting process stego object is obtained and extracted using stego key to discover the hidden message.
Steganography is classified into three main techniques; pure steganography, secret key steganography, and public key steganography [3]. In this study, research is focusing on the public key steganography. It is differ from pure and secret key steganography in the way it uses public and private key to secure electronic transmission between two parties [1]. Features-content of public key steganography is related to the components involved in public key steganography model. The components are domain which plays an important role in determining type of steganography function used, scheme which is steganographic function used for the embedding and extracting process and finally, evaluation parameters used for evaluating performance of the public key steganography application as a whole. Various evaluation parameters influence the quality of steganography model. Commonly, the significant of each parameter is depended on the PKS system goal [4].

Therefore, this paper offers review of PKS literatures based on different type of domain, schemes, and evaluation parameters applied over the last 6 years. It describes the trends of six steganography domains namely image, text, audio, video, multimedia messaging services, and transmission control protocol /internet protocol. It also highlights trends in public key steganography schemes and a few preferred evaluation parameters that are typically considered in public key steganography. This study aims to inspired further research in exploring the new least studied area or any potential in the area of public key steganography with better insight into potential algorithms and evaluation parameters that can be applied.
Organization of this paper is as follows. Section 2 provides the criteria used to review PKS system. Section 3 presents the outcome of the research based on literature papers. The result is presented in form of line graph to illustrate the trend of feature-content of PKS. Section 4 delivers the findings derived from the previous section in the form of preferred feature-content of PKS. Finally, our research work for this article is summarized in the last section.

2. Review Criteria

In reviewing PKS system, feature-content of PKS known as domain, scheme, and evaluation parameters are selected as a review criteria. For each criterion, there are corresponding types to be further discussed in this article

Copyright © 2016 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Table.1: Classification types on review criteria

Criteria	Types	Symbol Representation
Domain	Image	IM
	Audio	AU
	Video	VI
	Text	TXT
	Transmission Control Protocol/ Internet Protocol	TCP/IP
	Multimedia Messaging Services	MMS
Schemes	Rivest, Shamir, Adleman Algorithm	RSA
	Elliptical Curve Cryptography Algorithm	ECC
	Diffie-Hellman Key Exchange Protocol	DIF
	ElGamal Algorithm	ELG
	Digital Signature Algorithm	DSA
Evaluation parameters	Security	S
	Imperceptibility	I
	Capacity	C
	Robustness	R

Table 1 summarizes all the review criteria and its corresponding types. The symbol representation used as a character to represent the criteria types. Starting with the domain criteria, there are six types of domain namely image, audio, video, text, transmission control protocol/ internet protocol, and multimedia messaging services have been selected. The selection is based on the finding of the study where image, audio, video, and text are basic domain used in PKS while transmission control protocol/ internet protocol and multimedia messaging services are domain that just started to gain researcher's attention [5-7]. Secondly, the scheme criteria which identified from each PKS system employed; there are Rivest, Shamir, Adleman Algorithm, Elliptical Curve Cryptography Algorithm, Diffie-Hellman Key Exchange Protocol, ElGamal Algorithm, and Digital Signature Algorithm. These are among the widely used schemes in PKS [8-10]. Finally, the last review criterion is evaluation parameters which consist of security, imperceptibility, capacity, and robustness aspects. These evaluation parameters are identified based on the main goal of the authors in conducting their research work and those parameters are among the preferred evaluation parameters used in measuring the performance of PKS system [11-13].

3. Trends of Feature-content in Public Key Steganography

In this section, feature-content of PKS will be discussed in more detail based on the findings of our search for article on the subject of PKS. The discussion is explained in the form of feature-content of PKS trends. The trends are clustered into three categories; domain, scheme and evaluation parameter and presented in a form of line graph as illustrated in figure 2, 3 and 4.

In PKS, as formerly describe in pervious section there are six types of domains. Basic domains are IM, AU, VI, and TXT [5-7]. TCP/IP and MMS are two domains which lately started to raise attention in steganography area [6-7]. This might due to the advancement of current technology. As illustrated by the graph in Fig. 2, among the six domains, IM has clearly shown its popularity among the researchers by producing an upward trend since 2010. Although the number of PKS literatures found in IM is drop a bit during 2011 and 2014 but it still the most preferable domain. Meanwhile for AU and VI domain, PKS literatures produced in those two domains started to be found during 2012. And the numbers are fluctuated for AU domain. It hit the highest peak during 2014 where 5 literatures are found in the domain. As for VI, the numbers of literatures keep on increasing throughout the years except for 2013, no article able to be identified throughout the study. TXT is among the earliest medium used in steganography. However, in PKS, TXT domain is unpopular. Only one literature manages to be discovered in 2010 and 2011. And during the study, for 2012, 2013, and 2016, no literature is identified. The highest point for TXT is during 2014 with four literatures managed to be found.

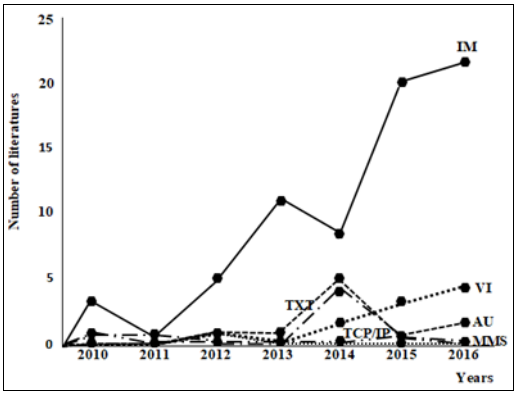


Fig.2: PKS domains trends

RSA, ECC, DIF, ELG, and DSA are schemes which widely applied in PKS area. The line graph in Fig. 3 shows the amount of each of the schemes applied in PKS literatures reviewed. It can be seen from the graph, RSA scheme has shown a rising trends throughout the years although the numbers drop a bit during 2014. The highest peak of RSA scheme is during 2016 found in PKS. Besides RSA, ECC is the second preferred scheme in PKS. However, in 2013 and backwards ECC scheme is still unpopular. It has shown a significant rise starting 2014 and onwards. In contrast to ECC and RSA, DIF, ELG, and DSA are the less preferred schemes in PKS. Amount of literatures found using these schemes in PKS are very limited and is it portrayed in the graph.

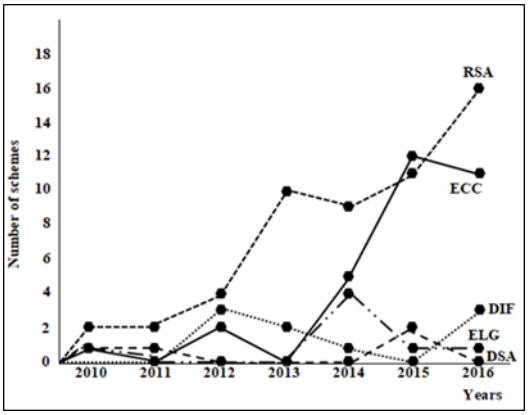


Fig.3: PKS scheme trends

Security, imperceptibility, capacity, and robustness aspects are the mostly used evaluation parameters in PKS literatures reviewed. The line chart in Fig. 4 depicts the amount for each parameter applied in the literatures. The most widely used evaluation parameter all the way through is security aspect. The period between 2012 and 2015 has shown a dramatic growth in the usage of security evaluation parameter. The numbers of security evaluation parameter applied as performance measurement reached a peak in 2015. Second preferred evaluation parameter is imperceptibility aspect. From 2010 to 2013 the number of imperceptibility evaluation parameter usage is remained static at approximately two literatures per year. However, it started to increase gradually from 2014 to 2016. Evaluation parameter of robustness and capacity aspects started to gain researchers attention in 2012. Numbers of

capacity evaluation parameter used has grown steadily throughout the years. As for robustness evaluation parameter, it is fluctuated

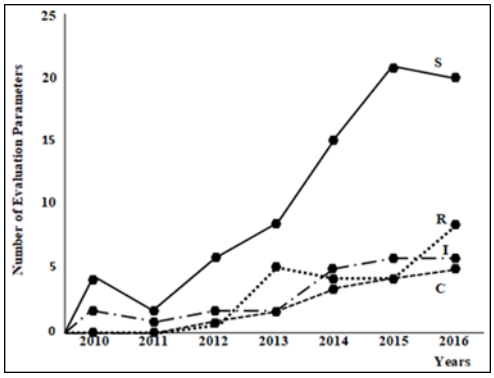


Fig.4: PKS evaluation parameters trends

4. Preferred Feature-content Criteria

The preferred feature-content criteria discussed in this segment is the finding retrieved from the trends discussed in the previous section. These preferred criteria are group and presented in accordance to domain, schemes and evaluation parameters aspects in a form of percentages.

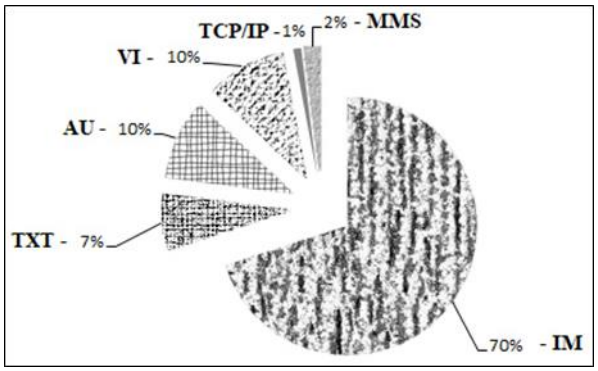


Fig.5: Preferred domain of PKS

As aforementioned, there are six domains in PKS namely IM, AU, VI, TXT, TCP/IP, and MMS. Based on the Fig. 5, it shows that majority of the literatures found are doing research in IM domain which contributed to 70% of the study. One major factor that leads to this finding is that image steganography is taking the advantages of limitation in human visual system (HVS) by tricking people to believe that no image manipulation has occurred [6][14]. Besides, this technique also becoming more popular recently due to overwhelming of electronic image information with the arrival of powerful technology in digital cameras and high speed internet distribution [13][15]. Having a huge amount of redundant data is another advantage of using image as a cover object [16]. As for AU, 10 literatures are found doing research in this domain and it has contributed 10% to the findings. Using audio file as a cover object is a very challenging task due to the sensitivity of human auditory system (HAS) [17][18]. Moreover, this technique also suffers to criticism such as limited amount of embedded data [13]. VI domain also contributes 10% to the findings of the study. This steganography technique is an extension of image steganography because it is a collection of still images and sometimes accompanied with audio. Beneficial of using this approach is the large amount of data can be embedded [19]. For this study, TXT domain has contributed 7% to the findings. It can be seen that this domain is less preferred compared to aforementioned domain. Using text as a cover object is a historic approach in steganography. Some researchers less preferred this technique due to very limited amount of redundant data which lead to limited hiding capacity [6][16][20]. Besides, text files also can be modified easily by unwanted parties which resulting to loss of hiding data [6][16]. Regardless of the limitations, some researchers still use text steganography because of smaller memory occupation and simpler communication [13]. Lastly, TCP/IP and MMS domain have contributed 1% and 2% to the finding of this study. Both of these steganography methods have significant contributions to the field of study.

Table.2: Preferred schemes of PKS

Domain	Schemes				
	RSA	**ECC**	**DIF**	**ELG**	**DSA**
IM	57.14	34.29	11.43	4.29	1.43
TXT	28.57	14.29	-	42.86	14.29
AU	80.00	-	-	10.00	10.00
VI	60.00	50.00	10.00	-	-
TCP/IP	-	100.00	-	-	-
MMS	-	100.00	-	-	-

Table.2. presents a finding of preferred scheme in accordance to domain. The percentage for each scheme is calculated based on specific domain. In IM, AU, and VI domain, most preferred scheme is RSA. It can be seen from the table where 57.14 % applied RSA in IM, 80% in AU and 60% in VI. The second preferred scheme in IM and VI domain is ECC which contributed by 34.29% and 50% to the finding. In TXT domain, preferred scheme is ELG with 42.86%. Meanwhile in TCP/IP and MMS domain, all the literatures found are doing research using ECC scheme.

Based on the outcome of the study displayed in the above table, it is proven that in asymmetric key algorithm, RSA is the most widely used and established scheme [8]. However, current situation demanding for high level of security and the use of simpler devices makes continued reliance on RSA is more challenging. And studies reveal that ECC scheme is an efficient alternative of RSA less power consumption and smaller key size [9]. As for the other schemes, each of them is having their own benefit and drawbacks [9]. It is up to the researcher to figure out the best fit scheme for their application.

Table.4: Preferred evaluation parameters of PKS

Domain	Evaluation Parameters			
	S	**I**	**C**	**R**
IM	74.29	20.00	17.14	24.29
TXT	57.14	71.43	57.14	14.29
AU	80.00	40.00	10.00	10.00
VI	100.00	30.00	20.00	30.00
TCP/IP	-	-	-	100.00
MMS	-	-	-	100.00

Finally, in Table.4, it lists the preferred evaluation parameters in accordance to domain. The finding shows that the most considered evaluation parameter in all domains is security aspect. 74.29% of security aspect is used in IM, 57.14% in TXT, 80% in AU, and 100% in VI domain. While in TCP/IP and MMS domain, all the literatures found applied robustness aspect which contributes 100% to the finding. Ideally, evaluation parameters applied in each application are vary depend on the requirement of the system. No application matches all the aspect of evaluation [21]. Some of these evaluation parameters conflict each other. According to Salomon [22], certain algorithm can only satisfy only one or two evaluation aspect. A secure steganography application can be developed by having a high degree of security or imperceptibility, while a high degree of capacity will produce a naïve steganography application and a high degree of robustness normally implemented in digital watermarking [22][23]. Researchers play an

important part in selecting the evaluation parameters in accordance to their system's goal.

5. Conclusion

Based on the analysis reviewed, it can be concluded that the most widely applied is image PKS domain. As for scheme's PKS trend, RSA and ECC have the highest demand to be applied in steganographic function. Finally, out of all evaluation parameter listed, the most popular evaluation parameter is security aspect. This review will be a useful material for other researchers to further up their study in exploring the least studied area in PKS or any potential area in feature-content of PKS.

Acknowledgement

This research was financially supported by the Research Grant Scheme, MoHE under RIMC Grant, Universiti Utara Malaysia.

References

[1] P. Kumar and V. K. Sharma, "Information Security Based on Steganography & Cryptography Techniques : A Review," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 4, no. 10, pp. 246–250, 2014.
[2] Rakhi and S. Gawande, "A Review on Steganography Methods," Int. J. Adv. Res. Electr. Electron. Instrum. Eng., vol. 2, no. 10, pp. 4635–4638, 2013.
[3] Z. K. Al-ani, A. A. Zaidan, B. B. Zaidan, and H. O. Alanazi, "Overview : Main Fundamentals for Steganography," J. Comput., vol. 2, no. 3, pp. 158–165, 2010.
[4] B. Zachariah, P. N. Yabuwat, and E. Bernard, "Application of Steganography and Cryptography for Secured Data Communication – A Review," Int. J. Eng. Res. Technol., vol. 5, no. 4, pp. 186–190, 2016
[5] J. Kour and D. Verma, "Steganography Techniques –A Review Paper," Int. J. Emerg. Res. Manag. &Technology, vol. 9359, no. 35, pp. 2278–9359, 2014.
[6] S. M. Thampi, "Information Hiding Techniques : A Tutorial Review," ISTE-STTP Netw. Secur. Cryptogr. LBSCE, 2004.
[7] M. Shirali-Shahreza, "Steganography in MMS," in 11th IEEE International Multitopic Conference, 2007, pp. 5–8.
[8] A. Sharma and N. Jain, "Steganography & Cryptography for Regimented Data Hiding System : A Review," Int. J. Sci. Res., vol. 4, no. 4, pp. 3119–3124, 2015.
[9] H. S and Dhamodharan R, "A Survey on DNA Based Cryptography using Differential Encryption and Decryption Algorithm," IOSR J. Electron. Commun. Eng. Ver. II, vol. 10, no. 5, pp. 2278–2834, 2015.
[10] P. P. Palsaniya and P. D. Soni, "CryptoSteganography : Security Enhancement by using Efficient Data Hiding Techniques," Int. J. Appl. or Innov. Eng. Manag., vol. 3, no. 2, pp. 263–267, 2014.
[11] R. Böhme, "Principles of Modern Steganography and Steganalysis," in Advanced Statistical Steganalysis, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 11–77.
[12] R. Maini, "A Comparitive Analysis of Steganography Techniques," pp. 67–70, 2016.
[13] R. Amirtharajan and J. B. B. Rayappan, "Steganography-time to time: A review," Res. J. Inf. Technol., vol. 5, no. 2, pp. 53–66, 2013.
[14] E. Zielińska, W. Mazurczyk, and K. Szczypiorski, "Development Trends in steganography," Commun. ACM, vol. 57, no. 3, pp. 86–95, 2014.
[15] N. Kaur and S. Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques," Int. J. Eng. Trends Technol., vol. 11, no. 8, pp. 388–392, 2014.
[16] M. M. Sadek, A. S. Khalifa, and M. G. M. Mostafa, "Video Steganography: A Comprehensive Review," Multimed. Tools Appl., vol. 74, no. 17, pp. 7063–7094, 2015.
[17] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," EURASIP J. Audio, Speech, Music Process., vol. 2012, no. 1, pp. 1–16, 2012.
[18] B. Zachariah, P. N. Yabuwat, and E. Bernard, "Application of Steganography and Cryptography for Secured Data Communication – A Review," Int. J. Eng. Res. Technol., vol. 5, no. 4, pp. 186–190, 2016.
[19] P. R. Kamble, P. S. Waghamode, V. S. Gaikwad, and M. G. B. Hogade, "Steganography Techniques: A Review," Int. J. Eng. Res. Technol., vol. 2, no. 10, pp. 3784–3793, 2013.
[20] H. Singh, P. Singh, and K. Saroha, "A Survey on Text Based Steganography," Proceedings of the 3rd National Conference; INDIA Com-2009 Computing For Nation Development. pp. 1–3, 2009.
[21] S. Kingslin and N. Kavitha, "Evaluative Approach towards Text Steganographic Techniques," Indian J. Sci. Technol., vol. 8, no. November, pp. 1–8, 2015.
[22] D. Salomon, "Data Hiding in Text," in Data Privacy and Security, New York, NY: Springer New York, 2003, pp. 245–267.
[23] D. Grībermans, A. Jeršovs, and P. Rusakovs, "Development of Requirements Specification for Steganographic Systems," Appl. Comput. Syst., vol. 20, no. 1, pp. 40–48, 2016