International Journal of Engineering & Technology, 7 (3.28) (2018) 17-19

SPC

International Journal of Engineering & Technology

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

Research paper

A conceptual model of tacit knowledge transfer in steganography

Noor Hasnita Abdul Talib[1*], Mazida Ahmad[2], Roshidi Din[2]

[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Malaysia
[2]School of Computing, College of Arts and Sciences, Universiti Utara Malaysia
**Corresponding author E-mail: nhasnita@kedah.uitm.edu.my*

Abstract

Steganography is a technique that involves a secret hidden message concealed inside the media cover using formats such as text, images, video or audio. Secret messages sent from the sender to the receiver are considered as knowledge being transferred from the expert to the novice. However, previous studies related to the knowledge transfer from experts to novices in the field of computer security, particularly in the field of steganography, are limited. Therefore, this study aims to investigate the knowledge transfer process occurring in steganography by using an information management transfer model. The methodology consists of theory development, model validation, instrument development, survey and model verification. This paper proposes a novel Stego-based SECI Model that demonstrates how the knowledge transfer process occurs in steganography.

Keywords: *Text steganography; information management transfer model.*

1. Introduction

Organizations face crucial challenges in retaining the knowledge of employees when they are leaving the organization [1]. These employees bring along their knowledge and expertise due to the difficulties in transferring expertise to other parties. This becomes a great loss for organizations because expertise and knowledge is considered an essential asset, and becomes the competitive advantage for the organization. As described by [2], it is essential to have Knowledge Management (KM) in place in order to ensure any intellectual assets are protected. Therefore, KM can be applied to create the processes and structures that create, capture, analyze and act upon information which allows transfer of knowledge to occur. KM has been widely implemented in organizations to improve efficiency, performance, and competitiveness. However, information security is mostly neglected from the KM perspective [3]. Therefore, it is vital to have the KM practices that take information security into account. The term security in data protection can be referred to as the preservation of confidentiality, integrity and availability of key attributes [4]. Information that requires protection can be hidden by using any information security methods such as encryption [5]. Other methods that can be used for information security are steganography, covert channels, anonymity and copyright marking [6]. Furthermore, there are numerous KM tools that require the transmission of data to novices such as via email.

According to [7], among the knowledge sharing technical barriers in organizations is an Information Technology (IT) system that does not sufficiently support the storage and sharing of explicit and tacit knowledge. The huge volume of data in the form of charts, graphs, presentations, voice mails and conversations leads to the overload of information and confusion for employees, unless it can be transformed to knowledge. In [8] state that “in the computer system, the weakest link has always been between the machine and humans because this bridge spans a space that begins with the physical and ends with the cognitive”. Therefore, several KM techniques can be applied in order to demonstrate how the knowledge creation process occurs such as using an SECI model, creative abrasion, parallel thinking or expert teams [9].

This research aims to investigate the relationship between KM SECI Model and steganography, which is among the techniques of hiding information. The SECI model was first introduced by [10] in the manufacturing industry. There are four main processes that can be used to convey tacit knowledge to novices. The first one is socialization, followed by an externalization process. Next is the combination and internalization process. The SECI model was also applied in the business sector, as well as government and non-governmental organizations [11].

On the other hand, steganography is a technique that hides a secret message in an ordinary message sent to the recipient. Hence, it prevents the original message from being intercepted by the unauthorized person which provides a safe exchange of information [12]. The remainder of the paper is organized as follows. Section 2 covers related work. Section 3 describes the new proposed model. The research methodology is discussed in Section 4, while the last section concludes this work.

2. Reviews

Many studies report the processes involved in managing knowledge within organizations. KM assumes that any individuals involved in the process of delivering and processing knowledge have relevant previous knowledge in their respective fields. Research in KM has been extended in many areas, especially in strategic management, system theory, organizational theory, organizational learning and artificial intelligence among others [13]. One particular aspect of Knowledge Management (KM) is knowledge transfer.

Knowledge transfer (KT) in organizations is defined as “the process through which one unit (e.g., group, department or division) is affected by the experience of another" [14]. According to [15], in the past 20 years, empirical research has shown that knowledge transfer in organizations may significantly improve knowledge and innovative capabilities. Two major types of knowledge are explicit knowledge and tacit knowledge [16]. Figure 1 shows four processes in the SECI model namely socialization, externalization, combination and internalization. Socialization is a process of expertise transfer from sender to receiver using methods such as email, forum space and sharing of experiences between experts and new employees in an organization. Secondly, externalization refers to the process of converting expert tacit knowledge into writing or explicit knowledge which can be shared with new employees who it as a base for a new knowledge. Next, Combination is the process of gathering inconsistent explicit knowledge to be compiled together in a more systematic form, e.g., in a manual book. Internalization is the process whereby the experience gained by novices is transformed into valuable useful knowledge that can be applied in the decision-making process and improve skills.

KM is also used in the field of information security. However, most studies focus on knowledge management in information security while very few studies focus on steganography. Many studies in information security adopt the knowledge transfer model to study user security awareness [17-18]. In [19] applied one knowledge transfer model as a method to understand the level of awareness and understanding of information security of real estate business employees. In [20] introduced a knowledge architecture for IT security (ISKA) to combine knowledge management principles and concepts so that organizations can determine their IT security knowledge based on three criteria: quality, completeness and effectiveness. As defined by [21], steganography is the practice of hiding a secret message within an ordinary message and the extraction of it at its destination. The ordinary message used for the secret message coverage is known as the cover message which can be in the form of text, image, video or audio. Steganography models consist of components such as secret messages, cover text, embedding algorithms, stego keys and recovering algorithms [22].

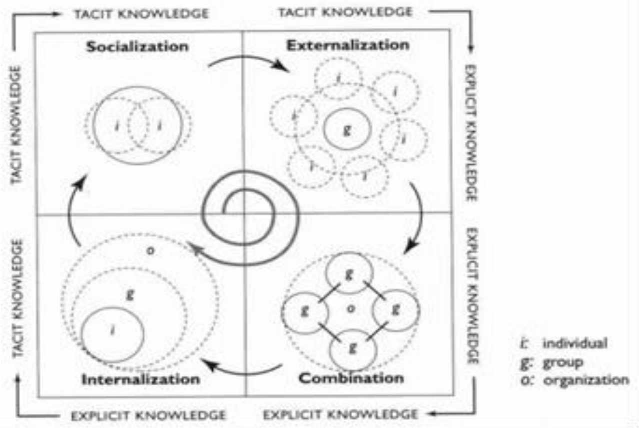

Fig. 1: SECI model [10]

3. The Proposed Conceptual Model

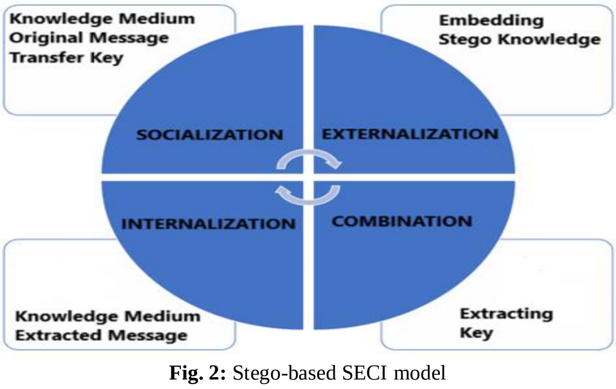

Fig. 2: Stego-based SECI model

The knowledge transfer model, referred to as SECI, has been used as a starting point for the proposed model. The proposed model is classified to four main groups namely Socialization (S), Externalization (E), Combination (C) and Internalization (I) as shown in Figure 2.

Steganography hides the existence of original messages (M), or hidden messages in the knowledge medium (C) or a cover text, so that third parties are unaware of their existence. The cover text is the original medium used before the message is embedded. The steganography process is safer with the use of the transfer keys (K), or keys before and after the sending of the message. Senders, or people with knowledge who want to share secret information with the receiver, will use steganography for discreet message sending. The receiver, or the novice, extracts the received message to read the secret information embedded in it, which will be used to improve their knowledge. Therefore, the entire process implies that the transfer of tacit knowledge of the sender to the receiver has occurred. In knowledge management, this process is called the process of socialization.

The embedding process is applied to modify the knowledge medium intended to embed original messages that produces stego knowledge (SK) or stego objects. Stego knowledge is the medium comprising the embedded message. This process uses the knowledge medium, the original message, and the transfer key as the sender's tacit knowledge to produce stego knowledge, which is the explicit knowledge. This process can be referred to as the externalization process.

The next process is Combination. The extracting process involves retrieving secret information from stego knowledge at the receiver's side. By integrating the key with the extracting (T) process, greater security will be enforced.

After the sender has received the extracted message, it becomes part of the receiver's knowledge, which becomes part of the assets for an organization. This is known as the Internalization process.

4. Discussion

There are five phases involved namely theory development, model validation, instrument development, survey and model verification as shown in Table 1.

In theory development, a careful reading is performed to gather information regarding knowledge transfer in the field of computer security/network, particularly in the field of steganography. The outcomes of this literature study are SECI processes, steganography components and the proposed conceptual model.

The next phase involves producing a mathematical formulation to verify the components involved in the tacit knowledge transfer of text steganography. The mathematical formulation is generated to determine the relationships among the components related to knowledge transfer in the field of steganography. In Instrument Development, mathematic formulations are converted into linguistic descriptions. The outcome is a list of linguistics descriptions.

Table 1: Research methodology

Phase	Activity	Outcomes
1	Theory Development • Construct Model	SECI processes Steganography components A proposed conceptual model
2	Model Validation Using Algorithm	A validated model using formal verification Relationships among the components
3	Instrument Development • Identify linguistic description	List of linguistics descriptions
4	Conduct Survey • Experimental/Expert Review	A validated model
5	Verify Model statistically • Survey	A verified model

The next step involves conducting a survey by using experiments and reviews from experts. The outcome is a validated model. The last process is the statistical verification of the model. The outcome is a verified stego-based SECI model.

5. Conclusion

Knowledge management is not widely applied in steganography. Thus, the main contribution of this study is to present a model of knowledge transfer in steganography by using a KM transfer model known as the SECI model which will enhance the understanding of the processes in tacit knowledge transfer. This model shows the knowledge creation within the steganography field. The steganography components are grouped in the four SECI main processes namely socialization, externalization, combination and internalization.

Acknowledgement

I would like to thank my respected guide Dr. Mazida Ahmad and Dr. Roshidi Din for their encouragement and support for the realization of this work.

References

[1] M. Arif and C. Egbu, "Measuring knowledge retention: A case study of a construction consultancy in the UAE," Eng. Constr. …, 2009.

[2] E. K. W. Lau, "Deploying the Measurement of Knowledge Management using the Balanced Scorecard," KMO 2016, 2016.

[3] S. Kesar, "Knowledge Management Within Information Security&#58; the Case of Barings Bank," Int. J. Bus. Inf. Syst., vol. 3, no. 6, pp. 652–667, 2008.

[4] K. Jairak, P. Praneetpolgrang, K. Jairak, P. Praneetpolgrang, C. Security, D. Systems, and C. Security, "Information Management and Computer Security Article information," 2013.

[5] J. J. C. H. Ryan, "Knowledge management needs security too," Vine, vol. 36, pp. 45–48, 2006.

[6] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - a survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.

[7] L. Bloice, S. Burnett, L. Bloice, and S. Burnett, "Barriers to knowledge sharing in third sector social care: A case study," J. Knowl. Manag., vol. 20, no. 1, pp. 125–145, 2016.

[8] A. S. McCampbell, L. M. Clare, and S. H. Gitters, "Knowledge management: The new challenge for the 21st century," J. Knowl. Manag., vol. 3, no. 3, pp. 172–179, 1999.

[9] P. Massingham and P. Massingham, "An evaluation of knowledge management tools: Part 1 – managing knowledge resources," 2014.

[10] I. Nonaka and H. Takeuchi, The knowledge-creating company: How Japanese companies create the dynamics of innovation. 1995.

[11] M. Nissen, "An extended model of knowledge-flow dynamics," Commun. Assoc. Inf. …, 2002.

[12] S. Chaudhary, M. Dave, A. Sanghi, and J. Manocha, "An Elucidation on Steganography and Cryptography," Proc. Second Int. Conf. Inf. Commun. Technol. Compet. Strateg., pp. 1–6, 2016.

[13] N. Hamid and J. Salim, "Exploring the role of transactive memory system (TMS) for knowledge transfer processes in Malaysia E-government IT outsourcing," Inf. Retr. Knowl. …, 2010.

[14] L. Argote and P. Ingram, "Knowledge transfer: A basis for competitive advantage in firms," Organ. Behav. Hum. Decis. …, 2000.

[15] M. Easterby-Smith, "Inter-organizational knowledge transfer: Current themes and future prospects," J. Manag. …, 2008.

[16] R. Williams, "Narratives of knowledge and intelligence beyond the tacit and explicit," J. Knowl. Manag., 2006.

[17] K. Thomson, R. von Solms, and L. Louw, "Cultivating an organizational information security culture," Comput. Fraud Secur., 2006.

[18] M. Siponen, "A conceptual foundation for organizational information security awareness," Inf. Manag. Comput. Secur., 2000.

[19] D. Mani, S. Mubarak, and K. Choo, "Understanding the Information Security Awareness Process in Real Estate Organizations Using the SECI Model," 20th Am. Conf., 2014.

[20] S. Kesh and P. Ratnasingam, "A knowledge architecture for IT security," Commun. ACM, 2007.

[21] S. Kumar, "Hiding the Text Messages of Variable Size using Encryption and Decryption Algorithms in Image Steganography," vol. 61, no. 6, pp. 47–52, 2013.

[22] M. G. Vennice, P. T. Rao, M. Swapna, and P. J. Sasi, "Hiding the Text Information using Stegnography," vol. 2, no. 1, pp. 126–131, 2012.