Information Sciences Letters

Volume 9
Issue 2 *May 2020*

Article 6

2020

StegoCrypto as Multi-Security Protocol to Ensure the Security Instance Messaging in the Sindhi Language

Munwar Ali
Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan, munwar.ali@sbbusba.edu.pk

Azeem Ayaz Mirani
Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan, munwar.ali@sbbusba.edu.pk

Reehan Ali Shah
Department of Computer Systems Engineering, Faculty of Engineering, The Islamia University Bahawalpur, Pakistan, munwar.ali@sbbusba.edu.pk

Asif Ali Wagan
Department of Computer Science, SMIU, Karachi, Pakistan, munwar.ali@sbbusba.edu.pk

Recommended Citation

Ali, Munwar; Ayaz Mirani, Azeem; Ali Shah, Reehan; and Ali Wagan, Asif (2020) "StegoCrypto as Multi-Security Protocol to Ensure the Security Instance Messaging in the Sindhi Language," *Information Sciences Letters*: Vol. 9 : Iss. 2 , Article 6.
Available at: https://digitalcommons.aaru.edu.jo/isl/vol9/iss2/6

Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/090206

StegoCrypto as Multi-Security Protocol to Ensure the Security Instance Messaging in the Sindhi Language

Munwar Ali[1,*], *Azeem Ayaz Mirani*[1], *Reehan Ali Shah*[2] *and Asif Ali Wagan*[3]

[1]Department of Information Technology, Shaheed Benazir Bhutto University, Shaheed Benazirabad, Sindh, Pakistan
[2]Department of Computer Systems Engineering, Faculty of Engineering, The Islamia University Bahawalpur, Pakistan
[3]Department of Computer Science, SMIU, Karachi, Pakistan

Received: 10 Oct. 2019, Revised: 28 March. 2020, Accepted: 10 April. 2020
ublished online: 1 May 2020

Abstract: Instance messaging services are an important source of communication among modern technology users. This kind of messaging service is also facing lots of security issues such as message breaching, confidentiality, integrity, availability, and interruption in communication. Few questions such as do existing security tools provide comfort to people? Or do existing security tools provide very basic protection that we believe that everybody needs? These questions need to answer in more detail and accurately. Due to the rapid development in technology, the way of communication is changed where the Internet provides the best way of communication among millions of people in the entire world. Nowadays users prefer to communicate in their local languages. Therefore the chances of communication breaches increase dramatically in local languages because negligible security-based work is done in many local languages. The majority of security-based work has been done in the English language but still, lots of work needs to be done on other languages including the Sindhi Language. In this paper, a new security model titled StegoCrypto is proposed to make more secure communication in the Sindhi language. The proposed StegoCrypto model is a hybrid of steganography and cryptography. It has been observed in the results that the proposed StegoCrypto model has succeeded in hiding the secret information in the text during communication between two users in the Sindhi language. To the best of our knowledge, this is the first kind of research done on the Sindhi language

Keywords: Steganography, cryptography, security, Sindhi text, secure communication.

1 Introduction

The way of communication changed with the advancement in digital media. According to a recent study, more than 4 billion people are Internet consumers and out of 4 billion 3.48 billion are social media users [1]. This way of communication does not only facilitates the users but also has introduced many new challenges for users. Security is one of the main challenges for technology users.

Different data security techniques are used to make secure communication among users. The most popular data security techniques are cryptography and steganography. Cryptography hides the text into unreadable text whereas Steganography is a Greek word coming from the cover text.''Stegano" means hidden and ''Graptos" means writing [2]. The use of steganography may vary from language to language. The majority of the population of the world uses the English language as the medium of communication. Due to the high number of users, the majority of the research work has been done on the English language to improve text communication security in English. Nowadays in almost everyone prefers to communicate in their native language on Internet/social media because they feel easy to communicate in their native languages. Therefore, it is very important to develop a security protocol to make secure communication in all languages. The Sindhi language is one of the oldest languages in the world. According to the latest statistics on Wikipedia, around 39 million are Sindhi speaking in the world [3]. The majority part of Sindhi speaker lives in Pakistan and India. Around 28.9 million people speak Sindhi in Pakistan and 2.7 million people speak the Sindhi language in India [3]. The Sindhi language contains a large number of Unicodes. It comprises 52 characters and each character has at least three formats and each format has its Unicode. The proposing and implementation of data security protocol in the Sindhi language is not easy. Therefore, the implementation of steganography varies from language to language because of different structures/forms of the letters of different languages. In this research, a new security

[*]Corresponding author mail: munwar.ali@sbbusba.edu.pk

protocol is proposed to secure instance text communication in the Sindhi language.

The rest of the paper is organized as follows. Section 2 describes the related work, section 3 describes the proposed StegoCrypto model, section 4 is about tools and technologies, section 5 presents the results obtained and the relevant discussions and finally, section 6 concludes this paper.

2 Literature Review

In computer science, hiding information needs a careful development of security algorithms. Information sharing is an important aspect of human language communication. Hiding secrete information in natural language format has been a greater part of research nowadays. The rapid growth of technology causes several threats like weak security, old security policies, unaware of the latest security breaches caused damage to personal and organizational destruction. Steganography is an art of hiding secret information from malicious. In 2014, efficient zero-width characters based steganography algorithm was developed for the Arabic language that deals with hiding one bit per letter [4]. The study focused on the high capacity media translation of the Arabic language. The transformation of a message with the limited length of the text is also a problem for long message communication. The length of a message with quality content hiding is an important issue in information hiding and cryptographic language translation.

A blood group-based steganography approach is used in [5]; where A, B, and AB groups are taken for connected doted, connected not-doted and separated Arabic characters respectively. Two stego options such as "kashida" and "change the Unicode" were used to get the best results as compared to some novel approaches.

In 2018, a stenographic algorithm was proposed that improved the length of the secrete message without losing message text [6]. Two different properties i.e. "Kashida" and small space text of the Arabic language has been considered as stego properties. These two properties can hide one bit by Kashida and three-bit by existing space. In the next year 2019, Khairullah et, al., in [7] proposed an efficient stenographic approach for the Bengali language through transliteration. The purpose was to exploit the special Bengali phonetic keyboard feature layout to hide the secret information. In the same year 2019, another study [8] conducted and proposed an efficient calligraphic algorithm that hides information using different phases such as embedding, extraction, and preparation.

The cryptography is a security technique widely used to secure data. For providing a secure and fast commination, several encryption techniques are introduced. In 2016, Ahmed et, al., [9] analyzed many encryption methods and it was observed that the end-to-end encryption is the most secure technique. In the year 2018, Endeley et.al., [10], proposed a new end-to-end messages encryption technique to provide secure messages to the end-user. Furthermore, the study also discussed different end-to-end security and privacy challenges in the light of government security policies.

Besides steganography, cryptography is the key tool to save electronic communication where email service is one of the famous electronic sources of sharing information. A comprehensive survey is conducted on secure email services presented in [11]. This survey focused on information security issues and threats that can be encountered in communication. The importance of the current enhancements in security for the exchange of data from a user to a user was also discussed. Threats like block recovery, message content modification, message forgery, denial of service and message interception are considered as the focused security threats related to email communication [12]. The Short Message Service (SMS) service of mobile technology is widely used by end-users. Call and SMS security issues are growing due to the huge utilization of mobile services. The study [13] focused on SMS security issues. The study overviews about current security trends in mobile SMS transformation. Cryptography techniques are implemented at the application layer level to develop an application based security service. However, network layer security issues are not focused on this study.

3 The Proposed StegoCrypto Model for Sindhi Text Communication

Lots of research work has been done on English, Arabic, Chinese and other languages but lots of research and struggle are required to work on the Sindhi language. Nowadays, the Sindhi language can easily be written in soft-form and also a major source of communication between people in Pakistan and India. Many studies have been conducted to make secure communication in the English language but as per our knowledge, there is not a single study conducted on secure communication in Sindhi. The secure communication between two parties in the Sindhi language is considered a core issue in this study. To solve such a research problem, the StegoCrypto protocol is developed which provides multi-layered security for Sindhi text communication. The proposed StegoCrypto protocol is divided into the following two security layers:

3.1 Security Layer 1

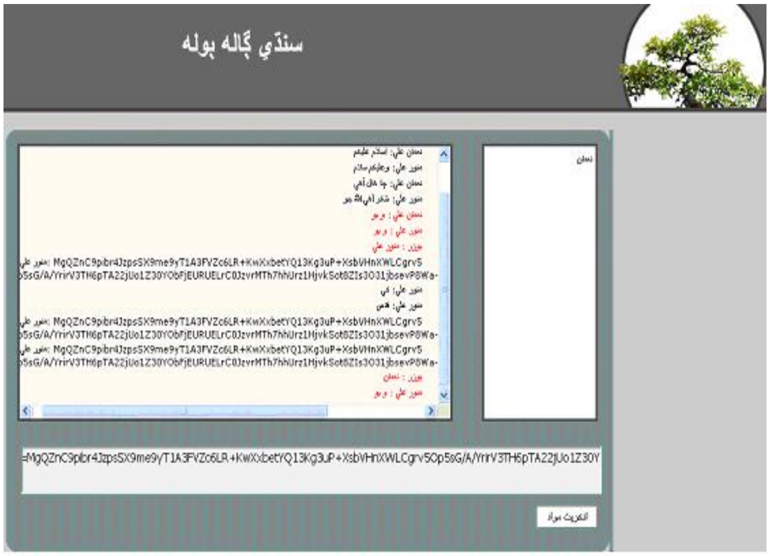
In this layer, steganography is used to hide confidential information in data from unauthorized users. In this study, steganography is used on the letter level. The Sindhi language consists of 52 letters and many letters in the Sindhi language has different forms. For steganography purposes, the letter Ain (ع) is considered. The main characteristic of letter Ain (ع) is its multiple-form nature. Letter Ain (ع) has four forms such as isolated (ع), final (ع), initial (عـ) and medial (ـعـ). The form of letter Ain depends on the position in the word. So, these forms of letter Ain (ع) are used to hide the specific information in data. In this proposed work, the particular position of Ain (ع) is changed to hide the information so that the third person/hacker should not identify the confidential message in data. To understand this procedure, an example is given here for clarification of the idea. Let's suppose that two parties are communicating with each other in Sindhi. The one wants to send the list of names in which few names are very confidential and the direct encryption is not the 100% security solution because the hacker can decrypt the encrypted data. So, firstly the confidential information is hidden with the steganography technique and later encrypted. The beauty of the steganography technique is that the information in readable format but difficult to identify which information is confidential/secret. Only the receiver and sender have the key to identify the secret information.

A list of names is given below. Sender A wants to send the list to the receiver B. The sender wants to keep name مسعود(Masood) as confidential and critical from unauthorized users. So, that the receiver should consider name مسعود(Masood) as some special name for security purposes or any other purpose. How to keep this name special and identifiable for the receiver and unidentifiable for hackers? Steganography is applied to answer this question. Through steganography, the medium form (ـعـ) of letter Ain is changed with initial form (عـ). This format changing makes a notable for the receiver but the hacker will just go through as a normal like other names in the list. The following example elaborates clearly.

For traditional readers, both list 1 and list 2 are the same and there is no difference and it is difficult to identify which name is kept secure because the name Masood is correctly written but the format of letter Ain (ع) is changed. So, if someone sends list 2 to the receiver and that message is hacked by a hacker, the hacker may be able to decrypt the first layer but would not be able to find the secret name in the list because it seems all public data in the list. A web application was developed to implement this concept as shown in figure 1.

مسعود → **Steganography** → مسعود

List-1	**List-2**
عليگل	عليگل
سميعالحق	سميعالحق
مسعود	مسعود
واسع	واسع
عاقب	عاقب



نعمان علي: اسلام عليڪم
منور علي: وعليڪم سلام
نعمان علي: ڇا حال آهي
منور علي: شڪر آهي الله جو
نعمان علي : ورچو
منور علي : ورچو
جوڙ : منور علي
منور علي: MgQZnC9pibr4JzpsSX9me9yT1A3FVZc6LR+KwXxbetYQ13Kg3uP+XsbVHnXWLCgrv5
5sG/A/YrirV3TH6pTA22jUo1Z30YObFjEURUELrC0JzvrMTh7hhUrz1HjvkSot8ZIs3O31jbsevP8Wa-
منور علي: ڪي
منور علي: هس
منور علي: MgQZnC9pibr4JzpsSX9me9yT1A3FVZc6LR+KwXxbetYQ13Kg3uP+XsbVHnXWLCgrv5
5sG/A/YrirV3TH6pTA22jUo1Z30YObFjEURUELrC0JzvrMTh7hhUrz1HjvkSot8ZIs3O31jbsevP8Wa-
منور علي: MgQZnC9pibr4JzpsSX9me9yT1A3FVZc6LR+KwXxbetYQ13Kg3uP+XsbVHnXWLCgrv5
5sG/A/YrirV3TH6pTA22jUo1Z30YObFjEURUELrC0JzvrMTh7hhUrz1HjvkSot8ZIs3O31jbsevP8Wa-
جوڙ : نعمان
منور علي : ورچو

=MgQZnC9pibr4JzpsSX9me9yT1A3FVZc6LR+KwXxbetYQ13Kg3uP+XsbVHnXWLCgrv5Op5sG/A/YrirV3TH6pTA22jUo1Z30Y

Fig. 1: View of Sindhi text messaging application.

In StegoCrypto model, the sender will write a message and can send to the receiver in three modes:

Send Plain text: The sender can send a plain text without applying any security tool.

Stego-text: Firstly, the sender selects the targeted letter of the word (need to be considered as a secret word) from the data/list; secondly, the letter format technique is applied, so the format of the letter is changed. Finally, we have stego version of the selected word. This mode is single layer security. This sender has a choice to skip the second layer of security and can apply only the first layer to save time, processing resources and network bandwidth.

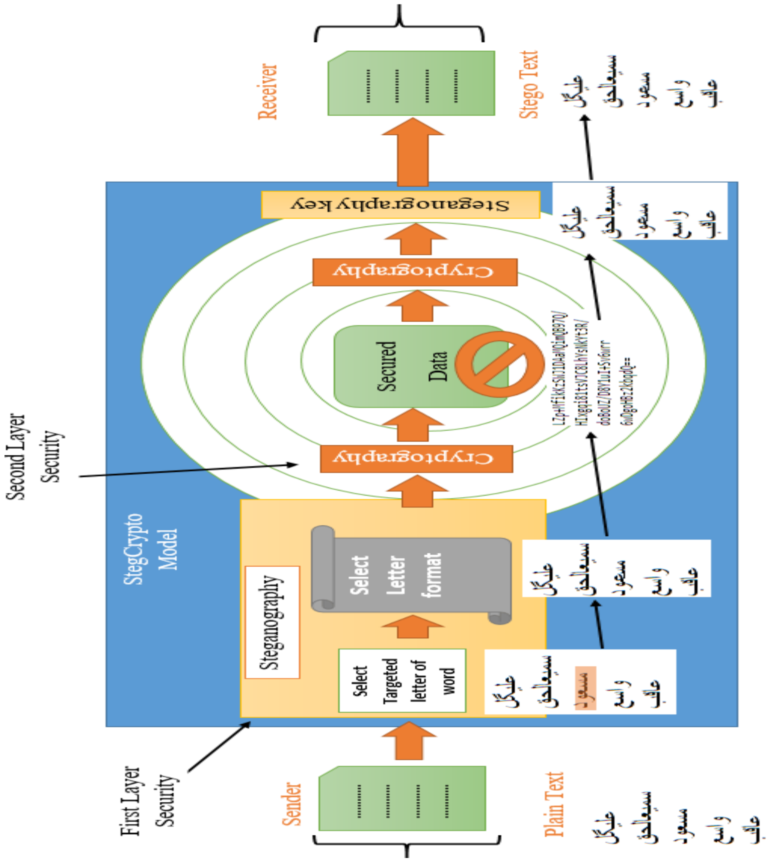


Fig. 2: Working process of the proposed StegoCrypto Model.

StegoCrypto-text: Send a text after applying steganography and cryptography techniques. Most confidential data is passed through both layers of security. First, steganography is applied to the plain text than cryptography is applied to make it more secure.

3.2 Security Layer 2

After applying steganography, the data encryption technique was applied to convert data into an unreadable format. For the encryption of stego-text, the RSA algorithm was used. The detailed working process of the proposed StegoCrypto model is also shown in figure 2.

4 Tools and Technologies

This software is developed in ASP.net using C # language. The basic purpose of this software is to provide a secure text communication to the Sindhi community.

5 Results and Discussions

A questionnaire was designed to ask the user to find the secret information in the data. The questionnaire given in appendix A. A very short questionnaire was designed to save the respondents time and to keep them motivated to complete the survey. The respondents for this survey are listed in table 1.

Table 1: Respondents of the questionnaire.

S. No.	Respondents
01	Faculty members / Teachers
02	Doctors
03	Engineers
04	IT Professionals
05	IT + Medical Students
06	Civil servants

In the survey, there was no gender discrimination, but all genders were given opportunity equally. In the list of respondents, response to the survey from male gender was high than female as shown in figure 3. Among all respondents, 79.8% were male and 20.2% were female; whereas few respondents did declare their gender.

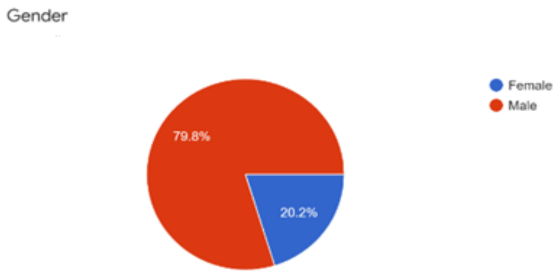
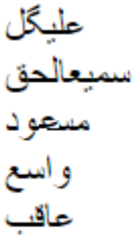


Fig. 3: Gender percentage of respondents.

To analyze the security strength of the proposed technique following the main question was asked from the respondents.

Do you see any hidden information in the data given below?


عليگل
سميعالحق
مسعود
واسع
عاقب

The main objective of this question was to get the feedback from respondents whether they can find the hidden information in stego-text given in the above question.

It has been observed from the responses of respondents that the majority of the people were unable to find the hidden information in the stego-text. In figure. 4, it is depicted that only 28.9% succeeded to identify the secret information in stego-text; whereas 16.3% of respondents were in double but even they could not figure out the secret information. The 14.7% of the respondents do not have any idea and they looked confused and few respondents did not choose any option from the given options. The majority of the respondents were unable to find the secret information from the first layer of the security i.e. stego-text. The ration is 38.4% who responded as "No" to the question, which shows that they were unable to find the secret information. Stego-text is in the readable format and all respondents can easily read the message but the majority of them are unable to detect the secret message enclosed in the text message. The person who has a steganography key will only be able to understand the secret message. For more details follow these steps to perform prescribed action.

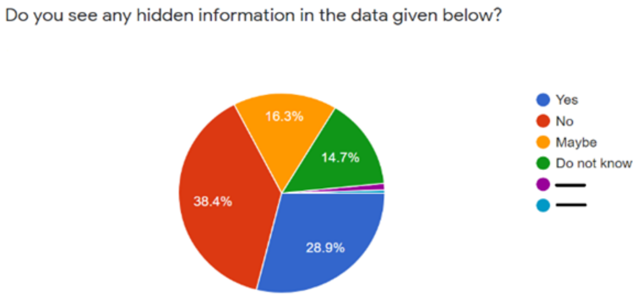


Fig. 4: Response regarding finding secret information in data.

6 Conclusions

A new stego-crypto technique was developed to provide secure text communication in the Sindhi language. The major part of this study was a text steganographic method for information hiding in text. This study was divided into two security layers i.e. steganographic layer and cryptography layer. In steganography, the secrete data is merged with text by changing the letter formats. The stego-text is readable to all users but difficult to find that the text contains a secret message. On the other side if someone noticed (which is a rare case) a small modification of letter in the text which may be considered typewriting errors by the sender. If encryption is broken but steganography will the secret information as secret. Therefore, the multi-layered proposed stego-crypto method is more reliable and secure. Moreover, the time of application is carefully selected to act in concert with the method of change and to improve safety.

References

[1] Digital 219: *Global Internet use accelerates*, by Simon Kemp, published at Wearesocial (2019) Link: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

[2] Kessler G, Hosmer C. *An overview of steganography.* Advan Comp 2011:83, ISSN: 0065-2458.

[3] Wikipedia: https://en.wikipedia.org/wiki/Sindhis

[4] Mohamed, A. A., An improved algorithm for information hiding based on features of Arabic text: A Unicode approach. *Egyptian Informatics Journal.*, **15,** 79-87 (2014)

[5] Malalla, S. and Shareef, F. R., A Novel Approach for Arabic Text Steganography Based on the "BloodGroup" Text Hiding Method. *Engineering Technology and Applied Science Research.*, **7(2)**, 1482–1485 (2017).

[6] Taha, A., Hammad, A. S., & Selim, M. M. A high capacity algorithm for information hiding in Arabic text. *Journal of King Saud University-Computer and Information Sciences* (2018). https://doi.org/10.1016/j.jksuci.2018.07.007

[7] Khairullah, M. A novel steganography method using transliteration of Bengali text. *Journal of King Saud University - Computer and Information Sciences.*, **31(3)**, 348–366 (2019).

[8] Hamzah, A. A., Khattab, S., and Bayomi, H., A linguistic steganography framework using Arabic calligraphy. *Journal of King Saud University - Computer and Information Sciences,*(2019). https://doi.org/10.1016/j.jksuci.2019.04.015

[9] Ahmed, H. M., and Khodher, M., Arabic Language Document Steganography Based On Huffman Code Using DRLR As (RNG), *Al-Mansour Journal*, **25**, 57–84 (2016).

[10] Endeley, R. E., End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. *Journal of Information Security*., **09(01)**, 95–99 (2018).

[11] Al-Mashhadi, H. M. and Alabiech, M. H., Survey of Email Service; Attacks, Security Methods and Protocols. *International Journal of Computer Applications.*, **162(11)**, 31–40 (2017).

[12] Choudhary, S. and Ghusinga, R., E-mail Security : Issues and Solutions, *International Journal of Computer Information Systems,* **7**, 42-46 (2013).

[13] Medani, A., Gani, A., Zakaria, O., Zaidan, A. A., and Zaidan, B. B., Review of mobile short message service security issues and techniques towards the solution. *Scientific Research and Essays.*, **6(6)**, 1147–1165 (2011).

Appendix-A: Questionnaire

The information is required for a research project only.

* Required

Gender *
Female
Male

Your Profession *

Your answer

Do you see any hidden information in the data given below? *

عليكل
سميعالحق
مسعود
واسع
عاقب

Yes
No
Maybe
Do not know
Other: