Robustness Analysis of a Steganography File Against a Media Sharing Process In Instant Messaging Applications

1st Putra Hadi Kamil [1],2nd Siti Ummi Masruroh[1], 3rd Nashrul Hakiem[1], 4th Frans Simangunsong[1], 5th Ashinta Sekar Bidari[1]
{putrahadi.kamil12@mhs.uinjkt.ac.id[1], ummi.masruroh@uinjkt.ac.id[1], hakiem@uinjkt.ac.id[1], frans@unsa@uinjkt.ac.id[1], ashintasb@unsa.ac.id[1]}

UIN Syarif Hidayatullah, Department of Informatics, Jakarta, Indonesia[1]

Abstract. The main challenge in digital communication is not only the need to share information but also to protect that information from attacks from irresponsible people, such as hackers. One method that effectively protects data is steganography. The application of steganography includes media such as images, audio, and video. The survey 'We are Social' in 2016 described the most widely used instant messaging applications in Indonesia as BlackBerry Messenger (BBM), WhatsApp, and Messenger. All these applications can be used for sharing media in the form of images, audio, and video, which means steganographic messages can be sent through these applications. However, in order to share media there is an inherent process of editing or compression of the files. This is one of the weaknesses of steganography. In this research, the authors will attempt a simulation by sending steganographic files of images, audio, and video through three instant messaging (BBM, WhatsApp, Messenger) applications. The results obtained indicate that the majority of steganographic files are lost after going through the sharing process, which means instant messaging applications are not suitable for use as media to send steganographic files.

Keywords: component; Steganography; Instant Messaging; Robustness; Sharing Media.

1 Introduction

Information technology is growing rapidly. Almost all methods of communication have changed into digital and to exchange information just using internet. However, there is a possibility that the information can be illegally taken and collected, transferred and used by others for their own interests. The main challenges faced in data privacy are the need to share information or data but also must protect the information against people who are not authorized to view such material, such as hackers. One method to protect data effectively is called steganography [1]. Steganography technique has been developed to hide a message in a picture or photograph. Steganography hide all the text information that only the sender and the recipient will be able to know that in the picture there is a hidden message. Some examples of steganography software are OpenPuff, OurSecret, S-Tools, Hide and Seek, and etc [2].

Based on the research conducted by WeAreSocial in their Digital, Social, and Mobile Report in 2016, the most widely used instant messaging application is the BlackBerry Messenger (BBM) at 19 %, the second is WhatsApp, followed by Messenger, Line and

ICONQUHAS 2018, October 02-04, Bandung, Indonesia

DOI 10.4108/eai.2-10-2018.2295574

WeChat [3]. The fifth application can be used to send images, audio, and video. In the sending process in those applications, there is a media compression process. One disadvantage of steganography in this case is the lack of robustness of the hidden data, as only a small attack, such as editing the picture and also the process of compressing the data may cause the hidden data to be corrupted or lost [4].

This research aims to analyse of a steganography file against a media sharing process in instant messaging applications (Whatsapp, Messenger, and Blackberry Messenger). The remainder of the paper is organized as follows. Section II describes literature review to this research and Section III shows briefly the experiment and the result. Section IV provides the conclusion of this paper.

2 Literature Review

2.1 Steganography

Steganography is a word derived from the Greek meaning "hide in plain sight". As defined by Cachin, steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganography techniques have been used for hundreds of years, but with the increasing use of files in an electronic format, new techniques for information hiding have become possible [5].

Steganography, encryption, and watermarking have been widely known and used to hide messages. Steganography is used to insert messages into another object called the cover or carrier. In cryptography, the sender of the message transforms plaintext into ciphertext using an encryption key and then the encrypted message is sent to the receiver. The receiver will change the ciphertext back into plaintext with the same key. In contrast, digital watermarking is a technique used to insert the information into images or other documents that can be seen or cannot be seen [6].

2.2 OpenPuff

OpenPuff is a steganography and watermarking tool that is well known and widely used. Open Puff was first developed by Cosimo Oliboni in 2012. OpenPuff grants a license as freeware under the Windows operating system. OpenPuff can hide data in multiple data types such as images, audio, and video. An Open puff carrier can combine multiple files to hide a secret message, which will make the message more difficult to decrypt illegally [7].

2.3 OurSecret

OurSecret is free software that can be used to hide secret information in images, audio, and video. OurSecret can be used to encrypt and hide secret messages in other files. In the first stage of using OurSecret the carrier determines the file and password to be used. Then, the secret message to be added will be inserted into the carrier [8].

2.4 Instant Messaging

In recent times, however, a new wave of mobile communications services called mobile instant messaging (MIM) applications have gained considerable momentum. Applications such as WhatsApp, BBM and Messenger allow mobile users to send real-time text messages to individuals or groups of friends at no cost. The third party application provides a messaging service for free to users either individually or as part of a group. This type of application has

arisen along with the development of many emerging smartphone technologies that support the development of many MIM applications [9].

2.5 WhatsApp

One example of a MIM application that is widely used is WhatsApp which is an instant messaging application that can be used on multiple platforms such as Android, iOS, Windows, and BlackBerry. WhatsApp makes it easy for users to communicate by sending messages that may include location information, images, audio and video in real-time and for free. At the time of writing, WhatsApp handles more than 10 billion messages per day and is one of the most popular cross-platform applications [9].

2.6 BBM

Another MIM application that is quite popular is the Blackberry Messenger (BBM). The Blackberry Messenger is a messaging application that is widely used on Blackberry devices. BBM requires users to exchange a pin to be able to communicate with it. BBM can also tell whether the messages are sent or read messages. In BBM users can exchange short messages, photos, video, or audio [10].

2.7 Messenger

One other MIM application that is widely used is Messenger or Facebook Messenger. All Facebook users can use this application. This application is not only able to send a short message, but is also able to send pictures, video, and audio, as well as location information and in addition can make free calls [11].

2.8 Related Work

The authors used several resources as literature sources based on earlier research. In [12], the research analysed the robustness of image steganography files after being sent through Facebook. This study also examined many tools of steganography, but only focused on images and one social media.

The research in [13] discussed tracing of steganography files in three social media applications (Facebook, Badoo, and Google+). This study also examined many tools of steganography, but only focused on images.

In [14] the study discussed image steganography in terms of sharing using social media applications. The research focused on improving security in steganography files. The deficiencies of this research are that it just focused on images and security and not on the robustness.

Based on previous research, the current authors will conduct research to analyse the robustness of a steganography file against a media sharing process in an instant messaging application. The purpose in performing this research is to determine the robustness of hidden messages in images, audio, and video after the sharing process via BBM, WhatsApp, and Messenger applications.

3 Experiment and Result

3.1 Input/Output Collection

This stage describes the input/output data used in this study.

Table 1. Secret Message

File	File Name	Size
.txt	Rahasia	7 bytes

Table I describes the secret message that will be used. The secret message used the .txt form with a size of 17 bytes named "Rahasia" (meaning "Secret" in the Indonesian language). The secret message is the message or information that will be inserted into the carrier file.

Table 2. Carrier File 1

File	File Name	File Type	Size
Image	Cute	.png	885KB
Image	easter	.bmp	351KB
Image	cat	.jpg	518KB
Audio	Simple	.mp3	2.82MB
Audio	Happy_	.wav	3.16MB
Video	Pigeons	.3gp	7.32MB
Video	Pigeons	.mp4	10.5MB

Table II describes Carrier File 1. There are three image files (PNG, BMP, JPG), two audio files (MP3, WAV), and two video files (3GP, MP4). The same secret message is inserted in every carrier file.

Table 3. Carrier File 2

File	File Name	File Type	Size
Image	Cartoon	.png	261KB
Image	Pooh	.bmp	538KB
Image	cartoonjpg	.jpg	109KB
Audio	minions	.mp3	993KB
Audio	cat meow	.wav	3.36MB
Video	Sponge	.3gp	9.9MB
Video	Sponge	.mp4	21.7MB

Table III describes carrier file 2. There are three image files (PNG, BMP, JPG), two audio files (MP3, WAV), and two video files (3GP, MP4). The same secret message is inserted in every carrier file. The difference between Carrier File 1 and Carrier File 2 is the size of the file.

3.2 Scenario I

In Scenario 1 the simulation involved sending the images via WhatsApp, Messenger, and BBM. The image formats were: JPEG, BMP, and PNG. The tool used to insert the secret message was Open Puff.

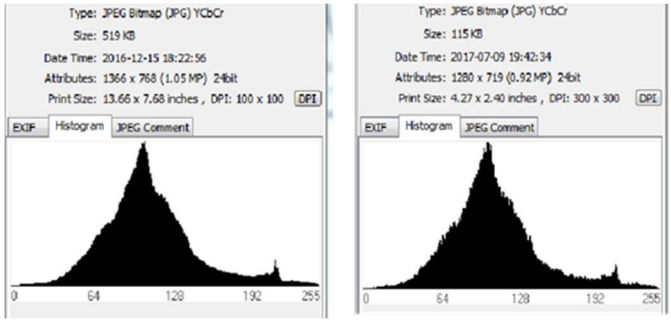
Table 4. Scenario 1 Result

File	File	Size	Secret

Name	Type		Message		
			WhatsApp	Messenger	BBM
Cute	.png	924KB	X	✓	x
easter	.bmp	351KB	X	x	x
cat	.jpg	518KB	X	x	x
Cartoon	.png	388KB	X	✓	x
Pooh	.bmp	538KB	X	x	x

x: Secret message missing, ✓: Secret message present

Table IV describes the results of Scenario 1, in which all the secret messages sent through WhatsApp were missing, while in Messenger only the PNG file in Carrier 1 and Carrier 2 preserved the message. For BBM only the JPEG file in Carrier 2 preserved the message. The format of the image files that were sent through WhatsApp all turned into JPEG format, while for BBM only the PNG files were changed to the JPEG format. In Messenger the format of all files was not affected.



a) Before Sending b) After Sending

Figure. 1. Image histogram before and after being sent through Whatsapp

Fig. 1 shows the difference that the left side (a) describes histogram of the image before being sent through Whatsapp, and the picture on the right (b) describes histogram of the image after being sent through Whatsapp. It is shown that the file size has been reduced, it is also that the quality of the image has been decreased which makes the secret message are missing.

3.3 Scenario 2

Scenario 2 simulated sending the image files via WhatsApp, Messenger, and BBM. The image formats were: JPEG, BMP, and PNG. The tool that was used to insert the secret message was OurSecret.

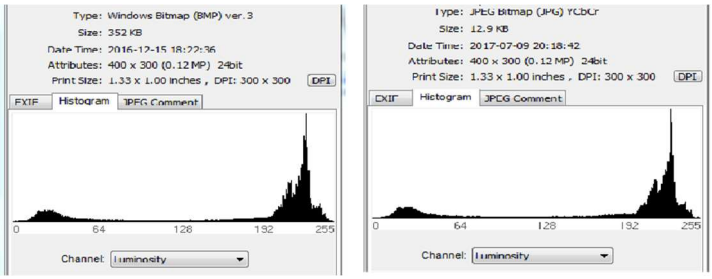
Table 4. Scenario 2 Result

File Name	File Type	Size	Secret Message		
			WhatsApp	Messenger	BBM
Cute	.png	924KB	x	x	x
easter	.bmp	351KB	x	x	x
cat	.jpg	518KB	x	x	x
Cartoon	.png	388KB	x	x	x

Pooh	.bmp	538KB	x	x	x

x: Secret message missing, ✓: Secret message present

Table V shows the results of Scenario 2 whereby all the secret messages sent through the WhatsApp, Messenger, and BBM applications were missing. The format of the image files that were sent through WhatsApp all turned into JPEG format. For BBM, only the PNG files were changed into the JPEG format, while in Messenger the format of all files remained unchanged.



a)Before Sending b) After Sending

Figure 2. Image histogram before and after being sent through Whatsapp

Figure 2 shows the difference that the left side (a) describes histogram of the image before being sent through Whatsapp, and the picture on the right (b) describes histogram of the image after being sent through Whatsapp. It is shown that the file size has been reduced, it is also that the quality of the image has been decreased which makes the secret message are missing.

3.4 Scenario 3

The simulation in Scenario 3 sent audio files via WhatsApp, Messenger, and BBM. There were two audio formats: MP3 and WAV. The tool that was used to insert the secret message was OpenPuff

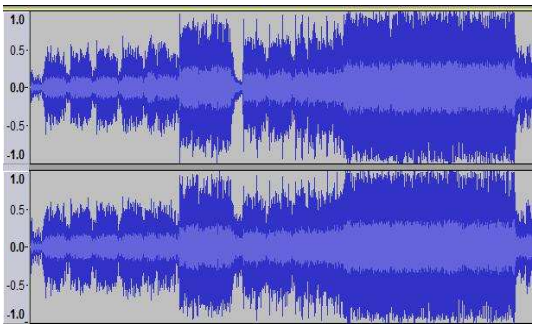
Table 6. Scenario 3 Result

File Name	File Type	Size	Secret Message		
			WhatsApp	Messenger	BBM
Simple	.mp3	2.82MB	✓	x	✓
Happy_	.wav	3.16MB	x	x	✓
Minions	.mp3	993KB	✓	x	✓
Cat meow	.wav	3.36MB	x	x	✓

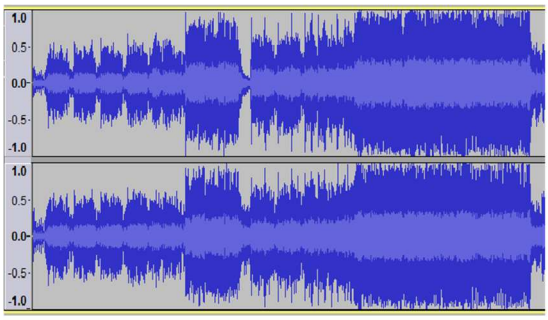
x: Secret message missing, ✓: Secret message present

Table VI describes the results of Scenario 3, in which all the secret messages sent through Messenger were missing because audio files cannot be downloaded but only heard via

streaming. . For WhatsApp the secret message was found in the MP3 file both in Carrier 1 and Carrier 2, while for BBM all the secret messages were found to be present.



a.) Before Sending



b.) After Sending

Figure 3. Audio spektogram before and after being sent through BBM

Figure 3 shows the difference that the left side (a) describes audio spektogram of the audio before being sent through BBM, and the picture on the right (b) describes audio spektogram of the audio after being sent through BBM. It shown that the audio file after being sent through BBM did not changed whether the quality or size. That's why all the secret messages were found to be present.

3.5 Scenario 4

In Scenario 4 the simulation sent an audio file via WhatsApp, Messenger, and BBM. There were two audio formats: MP3 and WAV. The tool that was used to insert the secret message was OurSecret.

formats: 3GP and MP4. The tool that was used to insert the secret message was OpenPuff.

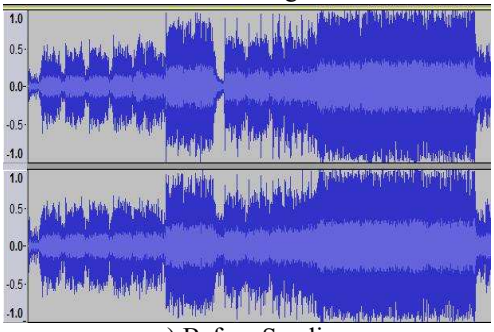
Table 7. Scenario 4 Result

File Name	File Type	Size	Secret Message		
			WhatsApp	Messenger	BBM

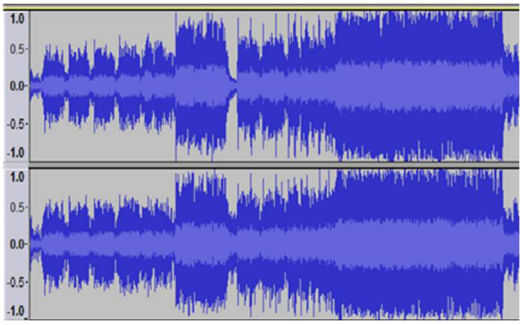
Simple	.mp3	2.82MB	✓	x	✓
Happy_	.wav	3.16MB	x	x	✓
Minions	.mp3	993KB	✓	x	✓
Cat meow	.wav	3.36MB	x	x	✓

x: Secret message missing, ✓: Secret message present

Table VII shows the results of Scenario 4. All the secret messages sent through Messenger were missing because audio files cannot be downloaded but only heard via streaming. For WhatsApp the secret message was found in the MP3 file both in Carrier 1 and Carrier 2, while for BBM all the secret messages remained intact.



a.) Before Sending



b.) After Sending

Figure 4. Audio before and after being sent through Whatsapp

Figure 4 shows the difference that the left side (a) describes audio spektogram of the audio before being sent through WhatsApp, and the picture on the right (b) describes audio spektogram of the audio after being sent through WhatsApp. It shown that the mp3 file after being sent through WhatsApp did not changed whether of quality or size. But all the wav file that were sent through WhatsApp all turned into .aac format, and makes the secret message are missing.

3.6 Scenario 5

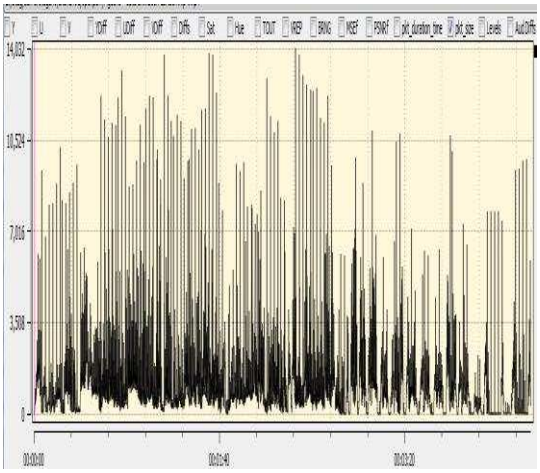
In Scenario 5 the simulation involved sending video files via WhatsApp, Messenger, and BBM. There were two video formats: 3GP and MP4. The tool that was used to insert the secret message was OpenPuff.

Table 8. Scenario 5 Result

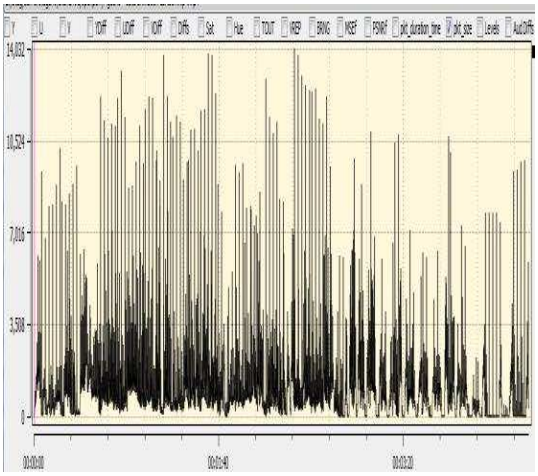
File Name	File Type	Size	Secret Message		
			WhatsApp	Messenger	BBM
Pigeons	.3gp	7.32MB	x	x	✓
Pigeons	.mp4	10.5MB	x	x	✓
Sponge	.3gp	9,9MB	x	x	✓
Sponge	.mp4	21,7MB	x	x	X

x: Secret message missing, ✓: Secret message present

Table VIII describes the results of Scenario 5. All the secret messages sent through Messenger were missing. For WhatsApp all video files could not be delivered, while for BBM all the secret messages were found to be present except for mp4 file in carrier 2, those file cannot be delivered because the file size is too big.



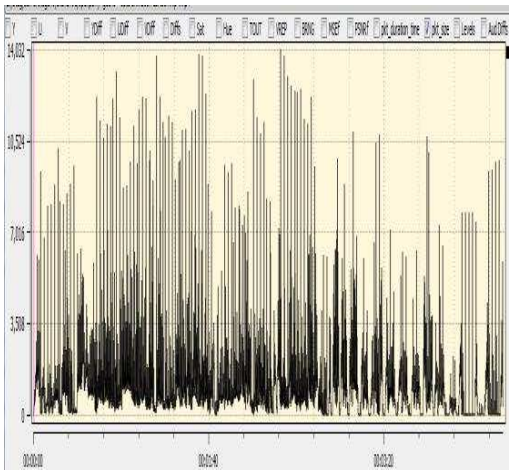
a.) Before Sending



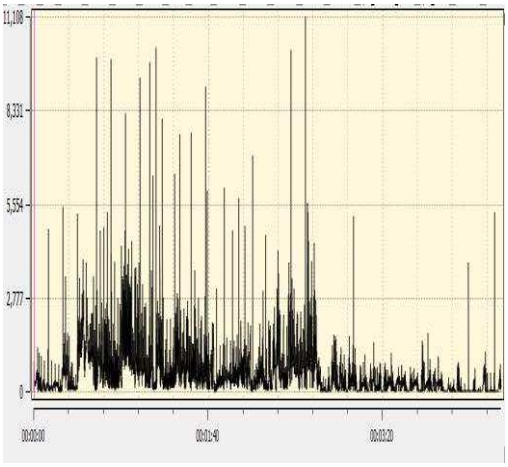
b.) After Sending

Figure 5. Video packet size before and after being sent through Messenger

Figure 5 shows the difference that the left side (a) describes video packet size before being sent through BBM, and the picture on the right (b) describes video packet size after being sent through BBM. It shown that the 3gp file after being sent through WhatsApp did not changed the quality. That's why all the secret messages were foung to be present.



a.) Before Sending



b.) After Sending

Figure 6. Video packet size before and after being sent through Messenger

Figure 6 shows the difference that the left side (a) describes video packet size before being sent through Messenger, and the picture on the right (b) describes video packet size after being sent through Messenger. It shown that the the video file after being sent through Messenger loss the quality. It makes all the secret messages sent through Messenger were missing.

3.7 Scenario 6

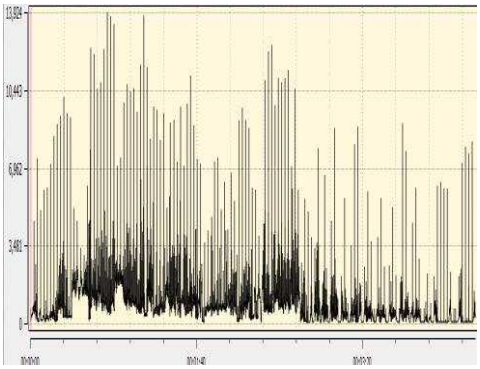
In Scenario 6 the simulation sent video files via WhatsApp, Messenger, and BBM. There were two audio formats: 3GP and MP4. The tool that was used to insert the secret message was OurSecret.

Table 9. Scenario 6 Result

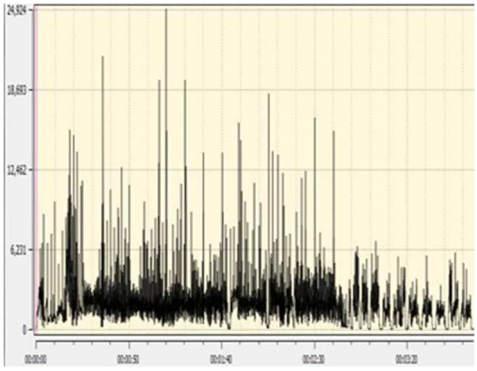
File Name	File Type	Size	Secret Message		
			WhatsApp	Messenger	BBM
Pigeons	.3gp	7.32MB	x	x	X
Pigeons	.mp4	10.5MB	x	x	X
Sponge	.3gp	9,9MB	x	x	X
Sponge	.mp4	21,7MB	x	x	X

x: Secret message missing, ✓: Secret message present

Table IX describes the results of Scenario 6. All the secret messages sent through WhatsApp, Messenger, and BBM applications were missing.



a.) Before Sending



b.) After Sending

Figure 7. Video packet size before and after being sent through BBM

Figure 7 shows the difference that the left side (a) describes video packet size before being sent through BBM, and the picture on the right (b) describes video packet size after being sent through BBM. It shown that the the video file after being sent through BBM have changed both of quality and size, and makes the secret messages are missing.

4 Conclusion

The conclusion of this research is as follows. Based on the results of the simulation work, the majority of secret messages which were inserted in pictures were lost when transmitted over instant messaging applications WhatsApp, Messenger, and BBM. This means that the robustness of image steganography sent via messaging applications is not good. PNG and BMP image files that were sent through WhatsApp and BBM were converted to the JPEG format. For the Messenger app, audio files could not be downloaded, as they can only be heard via streaming. For WhatsApp, if the secret message was inserted into a video file using OpenPuff, the video could not be sent. All the secret messages inserted in audio files sent using BBM were present when OpenPuff and OurSecret applications were used. Based on this study, the currently available instant messaging applications cannot be used as a tool to send secret messages by steganography because the majority of the secret messages will be lost.

Acknowledgements. This work was supported in part by the Institute for Research and Community Services (LP2M) UIN Syarif Hidayatullah Jakarta. This paper in conjuction with the 1st International Conference On Islam, Science, And Technology (ICONIST) 2018, Malang, East Java

References

[1] R. Rejani, D. Murugan, and D. V Krishnan, "Digital Data Protection Using Steganography," *ICTACT J. Commun. Technol.*, vol. 6948, no. March, pp. 1245–1254, 2016.

[2] S. Atawneh, A. Almomani, and P. Sumari, "Steganography in digital images: Common approaches and tools," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 30, no. March 2015, pp. 344– 358, 2013.

[3] D. Rosabel, "Digital in 2016 - We Are Social UK," 2016. [Online]. Available:http://wearesocial.com/uk/special-reports/digital-in-2016. [Accessed: 30-Jan-2017].

[4] M. H. and M. Hussain, "A Survey of Image Steganography Techniques," *Int. J. Adv. Sci. Technol.*, vol. 54, pp. 113–124, 2013.

[5] Cummin and Diskin, "Special Issue on Steganography and Digital Watermarking," *Network*, vol. 153, no. 3, pp. 2005–2006, 2004.

[6] H. V Desai, "Steganography , Cryptography , Watermarking : A Comparative Study," *J. Glob. Res. Comput. Sci.*, vol. 3, no. 12, pp. 2010–2012, 2012.

[7] T. Sloan and J. Hernandez-Castro, "Steganalysis of OpenPuff through atomic concatenation of MP4 flags," *Digit. Investig.*, vol. 13, no. June, pp. 15–21, 2015.

[8] S. M. Kunjir, S. D. Patil, S. Jabeen, S. V Bhosale, and D. Y. P. A. C. S. College, "Review On Stenography Tools," *Int. Res. J. Eng. Technol.*, vol. 3, no. 10, pp. 1223–1225, 2016.

[9] K. Church and R. Oliviera, "What's up with WhatsApp? Comparing Mobile Instant Messaging Behaviors with Traditional SMS," *Mob. HCI*, pp. 352–361, 2013.

[10] L. Reynolds *et al.*, "Contact Stratification and Deception: Blackberry Messenger versus SMS Use among Students," *CSCW '11*, pp. 221–224, 2011.

[11] "Messenger." [Online]. Available: https://www.messenger.com/. [Accessed: 30-Jan-2017].

[12] J. Hiney, T. Dakve, K. Szczypiorski, and K. Gaj, "Using Facebook for Image steganography," *Warsaw Univ. Technol.*, 2015.

[13] B. Cusack, "Steganographic Checks In Digital Forensic Investigation : A Social Networking Case," *Aust. Digit. Forensics Conf.*, pp. 44–51, 2013.

[14] F. Heriniaina and L. Xiaofeng, "Pictographic steganography based on social networking websites," *ACSIJ Adv. Comput. Sci.*, vol. 5, no. 1, p. 9, 2016.