ISSN 2277-3061

A Novel Approach Covert Channel for Secret Communications

Mariam Khader[1], Ali Hadi [2], Jalal Atoum[3]

Information System and Network Dept., World Islamic Science & Education University (WISE), Jordan

Mariam.S.Khader@gmail.com

Computer Science Dept., Princess Sumaya University for Technology (PSUT), Jordan

a.hadi@psut.edu.jo

Computer Science Dept., Princess Sumaya University for Technology (PSUT), Jordan

atoum@psut.edu.jo

ABSTRACT

This paper presents a novel covert channel for secret communications. It implements a new application layer covert channel, by applying multimedia steganography techniques to hide secret messages. This new channel method (called Under Your Radar (UYR)) provides a stealthiness method for the communication channel and an efficient method for hiding messages, as proved by our investigations. Such a covert channel will be used for transferring secret messages in two phases. In phase one, the message characters will be embedded randomly into the pixels of video frames. The choice of pixels is dependent on finding an identical value of the character ASCII representation from one of the pixel channels. The positions of pixels will form the steganography key, which will be used later to extract the message. Also, the steganography key will be embedded in an image using the LSB steganography technique. In phase two, the secret message will be exchanged between the sender and the receiver by sharing the video along with the steganography key over a public service (e.g. a social network), which serves as the new covert communication channel. The experiments outcomes have showed an improvement on the success of the proposed covert channel in exchanging secret messages without rising suspicion by observers or detection tools.

Keywords

Covert Channel; Steganography; LSB; Data Hiding; Social Network;.

Academic Discipline And Sub-Disciplines

Computer Science;

SUBJECT CLASSIFICATION

Information and Network Security

TYPE (METHOD/APPROACH)

Experimental research

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol. 14, No. 2

www.ijctonline.com , editorijctonline@gmail.com

ISSN 2277-3061

INTRODUCTION

The Life now is easier than before; the entire world is connected together through the magnificent world of the Internet. People are becoming more reliant on this world, where a tremendous number of applications and huge data travel over the Internet. This huge connectivity is now governing people purchases, bank transfers, communications and many other needs, that are done in such a sophisticated digital world. In spite of its magnificent, the Internet world has an opposite face of its magnificence, which is the risk of increasing of espionages and data thefts. Such attacks that are now developed with more intelligence and advanced techniques. This has called for the necessity for data hiding and developing new methods for secret communications. These methods have been used either for protecting data or by criminals to hide their communications [1].

Governments' agencies, criminals, companies and even individuals have an interest to keep their communications secret. And when thinking about having secret communications, all generally think about encryption. Encryption is the most efficient way to keep data from unauthorized disclosure, but the problem of using encryption is that it lures curious observers to obtain and to unravell the encrypted traffic. While encryption protects communication from being decoded, covert channels hide the fact that a communication is even exist. Covert channels use network protocols and applications as carriers for hidden messages, which makes channel detections more complex for observers, as there is no new connections or traffic generated. The huge amount of data and vast number of different protocols in the Internet provide a mean for high-bandwidth channels for covert communications [2]. These channels main goal is not to hide the transferred data but to hide the fact that there is data being sent. Nevertheless, combining encryption with this channel provides a better multilayer protection for hidden data [3].

Covert channels are more reliable and stealthy in covert important communications. Network administrators use these channels to hide network management data from hackers and Honeypots systems using the channels to export logged data in real-time that are hidden from the attacker. Also, covertness is used for transmitting authentication data [4].

COVERT CHANNELS BACKGROUND

Covert channel is defined as hiding of information in a way that prevents its detection. Covert channels have been applied in many different ways using TCP/IP layers: Network, IP, Transport and Application layer. These channels have evolved to use Protocol Encapsulation, Encrypted Protocols and Application Encapsulation. New techniques in covert channels are to apply application encapsulation over known applications such as: social networks, as it is the most used technique by people [5].

The desire of having complete security in open-systems environments (Internet) has increased the demand for new data hiding techniques, in order to overcome the lack of used encryption systems strength when used alone. The lack of available encryption technique is a result of political issues that restrict the efficiency of used encryption algorithms or that prevent using them at all! [6]. Also, for copyright protection, adding encipher copyright datum to the file could be easily stripped, but implementing datum within the file contents will prevent removing this datum [7].

Implementing a covert channel over public services means that even if a secret message is in a plain text; it will be strenuous even for conscious observer to notice that a message is being transmitted. The social network is considered the perfect medium for implementing the covert channel and hiding the secret message. Within its massive traffic compared with other existing techniques it is preferable, as it provides more stealth and reliability in hiding data [5].

Despite that there are many techniques for covert channels, using video steganography for secret messages is due to the rapid increase of exchanging video files over the Internet (which is predicted to increase exponentially over the next decade). The exchange of video files provides a typical cover for secret messages over other multimedia files [8]. Furthermore, the huge amount of data and vast number of different protocols transmitted over the Internet provide a high-bandwidth channel for covert communications and will make it hard to suspect the videos, pictures or users involved in the communication [9].

Seganography plays a major part in defending privacy for different applications. In the last decade there were many researches done on improving steganography applications that are used in: Online transactions, military communication, ownership of digital images, authentication, copyright, data integrity, adding captions to images, etc [10, 11]. In this research, video (multimedia) steganography is used as a media for our proposed covert channel due to the fast increase in movies shared over the Internet [8]. and due the fact that large sizes of video files allows larger set of data to be hidden than other available steganography techniques [11]

RESEARCH GOAL

The goal of this research is to create a new unobservable covert channel for secrete communication. In order to achieve a stealthier channel, the new covert channel is based on steganography and running over a public social network. The new covert channel utilizes the advantage of video steganography to conceal secret messages inside video files. Such video files will be already shared over the social network. Also, they will be used by communicated parties, either to embed or extract hidden messages from the shared videos.

For any covert channel, the following properties should be met [12]: The used channel should ensure Plausibility or Unobservability against either detection systems or observers. Also, it should be anonymous and ensure anonymity Set property. The technique should as well keep the Privacy of secret messages, so authentication and/or encoding could be added for more confidentiality. Finally, the user of the covert channel needs to ensure that the channel is Unlinkable [13]. If the channel could achieve the previous mentioned properties, it should be utilized to hide as much data as possible.

ISSN 2277-3061

The problem of implementing the covert channel on a public service depends on this service availability. But it is rarely happened for these services to be down. However, the access to YouTube or any online social network could be blocked, and this will stop our communication channel. In such cases, anonymizing proxies or any portable digital media could be employed to transfer the two videos to their intent recipient, such as: USB drive, or through legitimate but unmonitored network traffic such as email or peer-to-peer file transfer.

The compression issue that is implemented over images and videos results in change of media files bits, this may lead to losing some message characters. So, in order to mitigate this issue, there will be a restriction over the used video resolution to be 360p. Also, the sender has to use a specific resolution for the image used to share the stego-key.

METHODOLOGY

The increased number of sniffing and espionage attacks breaches the privacy of communications, which demands outstanding efforts and implementing multiple techniques to protect private data. These techniques have to avoid many alternate and devastating mechanisms used to mitigate or stop these channels. Hence, hiding the fact that a communication exists is considered the most intelligible solution to avoid such mechanism. Therefore, this research has been carried to create a new covert channel that is eligible to transfer adequate size of secret messages and imperceptible to detection methods.

The creation of our new covert channel has used YouTube as a public service to provide proof of concept. The channel will be used to exchange information between two parties, the involved parties whether the sender or the receiver will apply our new method to hide the information within a video. The video will be uploaded to the public service (YouTube) by the sender and the receiver will apply UYR proposed method to extract and identify the hidden message within this video.

Approach

Figure 1 illustrates the new approach of covert channel. This approach satisfies a high degree of stealthiness and at the same time hides a large quantity of data. Also, it works by hiding a message in a video file, without any alteration on the file itself, and then sharing this video using a public service along with a character map to extract the hidden message.

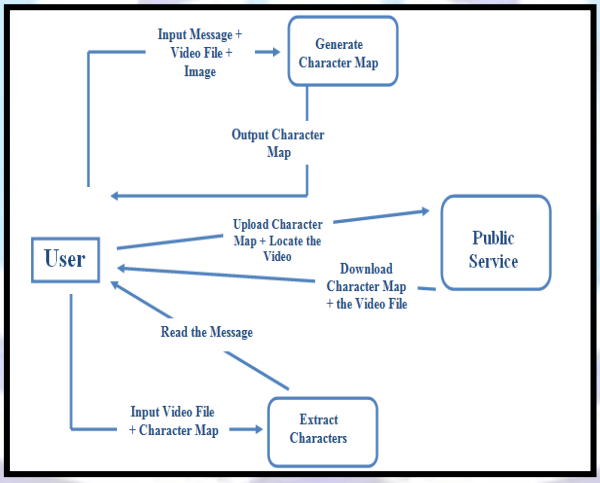

Fig1. An overview of UYR approach

This proposed approach of covert channel has a passive affect on the environment it works in. Implementing the covert channel within the application layer provides legitimate network traffic to hide data, thus it avoids generating any new traffic that may draw attention to the channel and may increase the traffic analysis efforts.

The video file used could be from a public service that shares videos (ex: YouTube) or any video file that the two communicating parties might agree upon. The message hiding process will generate a character map to be shared using either the same public service or another public service, based on their agreement. The character map is used to extract the hidden message from the video. The reason that video files were chosen as vessel to hide messages, is due to the enormous amount of video traffic traversing the network on a daily basis. Based on different high profile companies (Cisco, Google, Facebook, Twitter, etc) research, most Internet traffic by 2017 will be video traffic [13]. Also, using any video sharing website mitigates any direct transfer of the secret messages between the sender and receiver which guarantee unlinkability.

The process of generating the character map image (stego-key) will be done using virtual machines, and will be then shared with the second party using either the same or another public service. This will add another layer of anonymity to the communicating parties.

The steganography technique used in this research will make it strenuous to reveal the hidden message, because the video file has not been changed, so it is useless to analyze such a video for steganalysis or forensic investigation. Even if the observer got the image which includes the character map, he/she still needs to relate this map to the correct video used to generate the stego-key. This process is extremely strenuous when related to an active public video sharing website holding billions of videos and a network with such usual traffic traversing it. Besides that, there is no relation that relates the image to the video file.

Limitations

There are some issues that limit but not impede the usage of the proposed covert channel technique in hiding secret messages; these issues includes the data compression issue, which is used excessively on the Internet for multimedia files. As long as data will be lost due to a compression technique, there will always be a probability of losing secret message characters that are hidden within multimedia files contents. Hence, in order to avert such a loss, users of such a channel need to use PNG file format to store the character map, also, the chosen video to hide data need to be in specific size which is 360 pixel.

Another issue is that the size of the secret message should not exceed 65,000 bytes, this because of the limitation of the LSB technique that has been used to hide the character map. Anyway, this issue can be easily eliminated by adopting another technique to hide the character map.

There might be other issues that would appear depending on the agreement method between the sender and the receiver to share the character map. The Crop issue is an example, if the users agreement method was to share an image as a profile picture, they will be restricted to use a picture size of 255*255 pixels, to avoid data loss that could result from the Crop process.

Mutual Agreement

The process of sharing the video file and the character map is an important step before starting communication. For every message there will be a different video file and character map, the channel's users need to define a method to correlate the character map to its video file, this method needs to be unexpected.

After reviewing different known web-applications, it has been found that Google sites will serve the best as a proof of concept [5]. Firstly, there is no mechanism to check the account information validity (authentication), which provided from users that share this website, so the sender and the receiver accounts could easily be faked. Secondly, Google sites are considered the largest communities over the Internet. So, in this research, YouTube was used as a proof of concept, according to their website, the number of monthly visitors to this social network is more than one billion, also there are millions of subscription daily, and this number has increased four times since last year.

The Proposed Covert Channel Methodology

The proposed covert channel is illustrated in Figure 2. It utilizes the public service websites and multimedia steganography to hide secret messages, meanwhile providing a large container to hide data. The application layer covert channel is considered to be the most difficult to be detected, this is due to the fact that a huge number of applications used over the Internet and each application requiring a specific method to prevent or even detect covert channel existence.

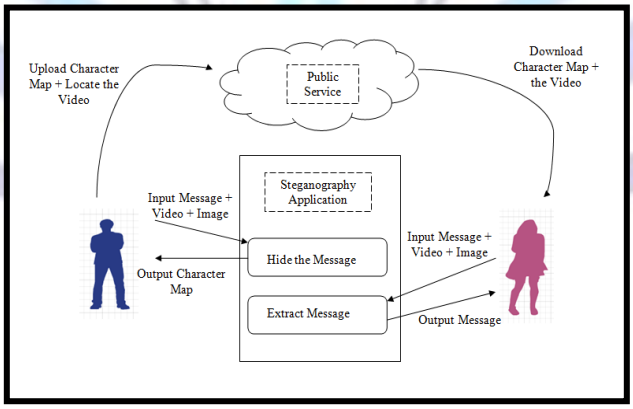

Fig2. An overview of the Proposed Covert Channel

The process of transferring a secret message will be done in two phases: Phase one, this phase is responsible for hiding the message characters in a video file (stego-file) and generating a character map image (stego-key) to extract the message by the received party. Phase two, this phase is responsible for sharing the video file (stego-file) along with the character map image (stego-key) through a public service, were the received party can download both (video file and image) and extract the message. In the next subsections the processes in each phase will be described in more details, using two partners Bob and Alice to communicate.

ISSN 2277-3061

1. Hiding The Message

Before Bob can use the new Covert Channel, the message must be hidden before it is sent to Alice. This will be done in three steps as follows:

Step-1: Input the Message

The first step to be done is providing the message to be sent by Bob. This will be achieved by the new covert channel application implemented as a proof of concept. The application will require Bob to input the message, and according to this message length the application will calculate the minimum length for the video that will be used to hide the message characters. Also, Bob will be asked to input the video file, which will serve as the stego-file and as the image, which will serve as the stego-key. This video file should be of a specific resolution that is known for Alice (to avoid compression loss issues).

Step-2: Choosing The Video File

The application will start searching YouTube for a video file that is long enough to hide the message. After BOB download the stego-file, Bob will use this video file as input to the new covert channel.

Step-3: Generating The Character Map

The new covert channel will search the downloaded video file (stego-file) to generate the character map (stego-key) to be hidden within the supplied image. The video will be read, transformed into a number of frames, as shown in Fig. 3.

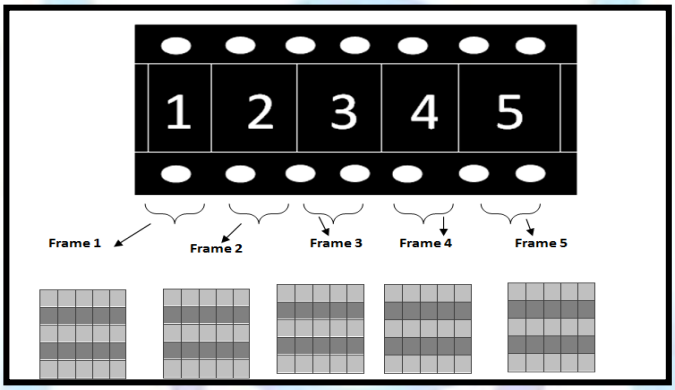

Fig3. Extracting Video Frames.

The UYR will embed the message characters inside the extracted frames. Each frame will be searched for a letter of the message, as shown in Fig. 4. This is done by searching for the identical byte value of message charters ASCII representation within the frame pixels value. Because the search process depends on the message characters, in every sent message a different character map will be generated that is dependent on the message itself. This helps to avoid specific pattern of embedding which is used in steganalysis techniques to detect hidden messages.

When the position of the character is found it will be retrieved along with the frame number to be used in generating the stego-key. The stego-key (as shown in Fig. 5) is a list of mapping from frame numbers to characters, which will be used later by Alice to extract the message.

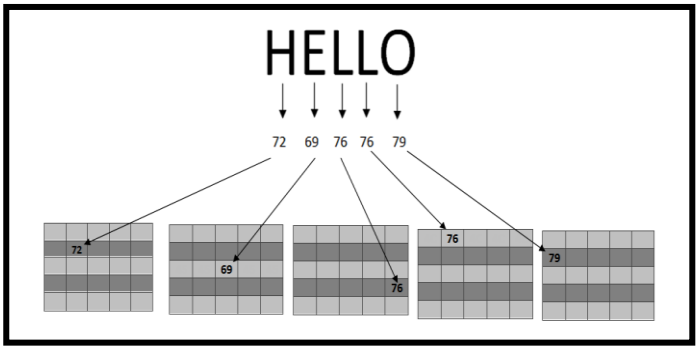

Fig4. Searching for Character Identical Values.

ISSN 2277-3061

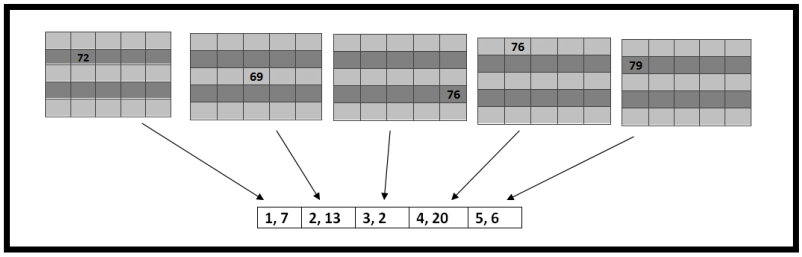

Fig5. Forming the Positions List, Frame Number and Position of Character.

Before hiding the stego-key within the sent image, a simple kind of obfuscation will be added to the key, as shown in Fig. 6. This is done by calculating the sum of each character mapping in the list and its position number in that list, to create the final character map (stego-key). The stego-key will be embedded using the LSB technique. The reason of using LSB technique is because it could be easily integrated into the proposed covert channel implementation.

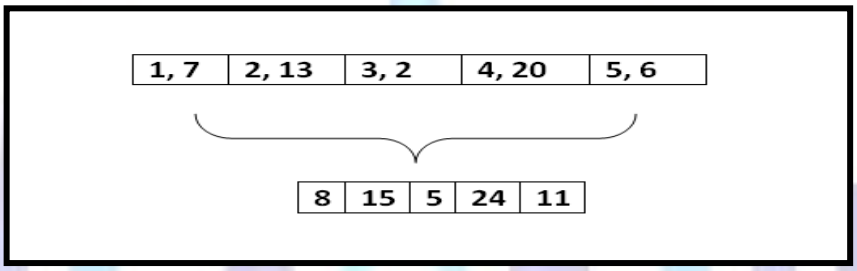

Figure6. Obfuscation by Adding the Position to the Frame Number.

The added obfuscation layer will help in case that the image is analyzed in steganalysis technique. Desipte that the analyzer would be able to extract the hidden data in this image, all what he will find is a sequence of numbers, and there will be no proof or correlation between this image and the newly Covert Channel implemented.

2. Upload Character Map

According to the mutual agreement between Alice and Bob; Bob now will send the character map and the video link to Alice. The PNG format is used to hide the stego-key, because it guarantees that no data will be lost due to any compression issues. Also, the communicating parties should be careful in the case that the image might be modified due to other factors during its transfer, such as: Resize - Cropping, Resampling and Scaling, as all of these techniques may result in data loss.

3. Extracting the Hidden Message

In this phase Alice will use the new covert channel to extract the message sent by Bob. This will be done in two steps as follows:

Step.1 Download Video File and Character Map

According to the mutual agreement, Alice will be notified about the new message, so she can download the video file (stego-file) and the character map image (stego-key) to use them by this covert channel to extract the hidden message characters.

Step.2 Extracting The Message Characters

In order to extract the message, Alice will use the same files; the same video file and character map image. The implemented covert channel will extract the frames from the stego-file. Then extract the position list from the stego-key. Based on this extracted information, the mapping between the frame numbers and the character positions will be generated, and saved into a list. This list will be used to deobfuscate the original character map, which is the exact byte locations and their frame numbers. Finally, the deofuscated character map will be used to retrieve the ASCII representations of the characters from the frames. This will form the final message sent by Bob to Alice.

EVALUATION

In order to evaluate the proposed covert channel, first we need to consider the basic criteria that any covert channel is built on it; this includes plausibility of the channel, which could be proven by evading detection mechanisms.

For any detection system and observer of the traffic, there should be a pattern in behavior or anomaly that is generated from the traffic on the covert channel to detect its existence, wherease, the proposed covert channel depends on its operation on the regular and legitimate traffic data (notifications). For example, sharing the character map could be done by changing the profile picture on Google+, which is being considred as a legitimate procedure, done frequently and has no limitation to change. In addition, it will be very strenuous to set a detection mechanism over profile pictures, because of the enormous number of users over social networks, so these pictures might only be examined when there is an obvious suspicious over this picture. The same goes with the video file; the sender will only add “Like” or share its link which is legitimate too, but whatever was the action, there is no proof that this video is a part of this communication, as it has not been altered at all!

The extreme traffic add anonymity to the channel, also, because of the huge number of users that increases the anonymity set of the channel. Besides these facts, the main strength in this covert channel technique is the strenuous to correlate a character map to its video file, since there is no relation between those two files, especially in an active video sharing website. Also, the channel achieves unlinkability for users, because even if the profile is known to send covert channels it is strenuous to know the other party, as there are no connections between the two parties. Unlinkability also is guaranteed for the channel as it depends on inserting its communication in legitimate data (Notifications). Finally, even though that the capacity of a shared message is limited in the implementation of this research, this is due to the LSB technique limitation, the capacity can be enlarged using another technique.

CONCLUSION

This paper has presented a new application covert channel layer for hiding communication messages between two parties. The new covert channel is implemented using Video and Image Steganographic techniques. The steganographic techniques were used to hide the message, which then would be shared over a public service. The implemented covert channel had achieved stealthiness, plausibility, anonymity, and unlinkability by:

First, there is no new traffic that has been generated by this proposed covert channel’s communication. No detection system could easily detect the existence of the communication channel, because it’s extremely hard to correlate between the video and image used to hide the message that is shared over the network.

Second, the used steganographic technique leaves no fingerprint within the files they have been applied to, which helps in avoiding detection systems that search for such fingerprints.

Also, utilizing a legitimate social network notifications used in public service websites, the message is encapsulated into normal data streams (videos and images), which makes it difficult to distinguish between the covert channel’s traffic and regular traffic.

Finally, as a proof of concept, the covert channel in this research has been implemented over a social networks (namely; YouTube) due to its huge daily number of users. This provides a perfect cover to increase the anonymity and anonymity set of the channel and it’s communicating parties, thus increasing the channel’s anonymity.

Future Work

Since every video that is watched on YouTube will be downloaded as a temporary file on the system, the steganography application can benefit from this temporary file to create the character map or to use it for extracting the hidden message, so the user doesn’t have to download the video again.

The proposed technique could be easily modified to add another feature of hiding images and binary files not only text messages.

Furthermore, there should be more efforts also to develop a new method of finding identical of the characters in any given frame, even if it contains limited range of values.

Another future work to consider, is adding other steganographic techniques to be used.

Finally, other considerations should be taken into account when developing covert channels such as the Image type, Video type, and the used public service.

REFERENCES

[1] S. Falesh, A. Dongre, and P. Soni. 2014. Comparison of different techniques for Steganography in images. International Journal of Application or Innovation in Engineering & Management (IJAIEM). vol. 3, no.2, pp. 171-176.

[2] S. Davidoff and J. Ham. 2012. Network Tunneling, Network Forensics: Tracking Hackers through Cyberspace, 1st ed. New Jersey:Pearson Education , pp. 423-460.

[3] E. Couture. Covert Channels. 2010. SANS Institute: InfoSec Reading Room.

[4] H. Al-Bahadili, and A. H. Hadi. 2010 . Network Security Using Hybrid Port Knocking." IJCSNS International Journal of Computer Science and Network Security. vol.10, no.8, pp. 8-12.

[5] J. Selvi. 2012. Covert Channels over Social Network. SANS Institute: InfoSec Reading Room.

[6] B. Dunbar. 2002. A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment. SANS Institute: InfoSec Reading Room.

[7] H. .A. Jalab, A. A. Zaidan and B.B. Zaidan. 2009. Frame Selected Approach for Hiding Data within MPEG Video Using Bit Plane Complexity Segmentation. Journal of Computing. vol. 1, no.1, pp. 108-113.

[8] VisualApogee. 2014. Online Video Impact in 2014," http://visual.ly/online-video-impact-2014?utm_source=visually_embed.

[9] S. Zander, G. Armitage , and P. Branch. 2014. Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Communications, vol. 3, no.2 , pp. 171-176.

[10] A. Al-Farajat, H. Jalab, Z. Kasirun and B. Zaidan. 2010. Hiding Data in Video File: An Overview. Journal of Applied Sciences. vol. 10, no.1, pp.1644-1649.

[11] M. Garg and G. Jangra. 2014. An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques." International Journal of Advanced Research in Computer Science and Software Engineering). vol. 4, no.1, pp. 746-751.

[12] R. Sbrusch. 2006. Network Covert Channels: Subversive Secrecy." SANS Institute: InfoSec Reading Room.

[13] M. Smeets, M. Koot. 2006. Research Report: Covert Channels." University of Amsterdam, vol. 3, no.2.

BIOGRAPHY

Mariam Khader She received the B.S. degree in computer networking systems from the World Islamic Science and Education University (WISE), Amman, Jordan, in 2012, and the M.S. degree in IT security and digital criminology from Princess Sumaya University (PSUT), Amman, Jordan, in 2014. She is CCNA certified. Since 2012, she has been working at the Department of Computer Network, WISE University, in Amman, Jordan as a Teacher Assistance (now Lecturer). Her current research interests include computer forensics, malware analysis and network security.

Dr. Ali Hadi received the B.S. degree in computer science from Philadelphia University, Amman, Jordan, in 2002 and the M.S. and Ph.D. degree in computer information system from University of Banking and Financial Sciences, College of Information Technology, Amman, Jordan, in 2004 and 2010, respectively. He was a system and security engineer for different high reputed companies from 1998 to 2011. He was an Assistant Professor with the Business Networking and Systems Management Department at Philadelphia University from 2011 to 2014. Since 2012, he was a visited lecturer (now full time) in the Computer Science Dept., King Hussein Faculty of Computing Sciences at Princess Sumaya University for Technology (PSUT). He is the author of two book chapters, more than 100 articles. His research interests include digital forensics, operating systems internals, malware analysis, and network security. Dr. Hadi throughout his professional career gained more than 14 well known technical certificates (OSCP, CHFI, CEH, RHCE, Novell CLP, etc).

Prof. Jalal Atoum is currently the Vice President at Princess Sumaya University for Technology (PSUT). He had received his B.S. degree in computer science from Yarmouk university-Jordan in 1984. He had received his Master degree in computer science from University of Texas at Arlington-USA in 1987. He had received his PhD in computer science from University of Houston-USA in 1993. He had worked as an assistant professor at Yarmouk University from 1993 to 1995. He had been appointed as the Computer Science department Chairman at PSUT. He has supervised or co-supervised several students on their Ph.D. dissertations and several M.S. theses and has supervised numerous undergraduate graduation projects. Finally, he have been involved in several committees for degree plans, proposed and developed the Master program in Information System Security and Digital Criminology at PSUT.