Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 10 (16): 1825-1833, 2010
ISSN 1812-5654

On the Capacity and Security of Steganography Approaches: An Overview

[1]Ali K. Hmood, [1]Hamid A. Jalab, [1]Z.M. Kasirun, [2]B.B. Zaidan and [2]A.A. Zaidan
[1]Faculty of Computer Science and Information Technology,
University of Malaya, 50603, Kuala Lumpur, Malaysia
[2]Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Selangor Darul Ehsan, Malaysia

Abstract: The aim of this study is to review the strength and weakness for the possible multimedia cover for the steganography approaches. In addition, the security level of each approach and how is probable to combine the steganography and cryptography. Steganography is an art on which the data can be hide in other data as cover, the multimedia files is the commonly used for hiding data. The main aspects of the steganography is the capacity and security, where the capacity refer to how much data can be hidden in the cover carrier, while the security concern with the ability of disclose or altering the data by unauthorized party. The multimedia files, such as, image, video, audio and text are the possible covers for hiding secure information or data. Each of these covers has advantages and disadvantages; as a result of this study we will discuss the possibility to use these files as a cover. In the last part of this study, we suggest a further direction to improve the capacity and security aspects.

Key words: Data hidden, steganography, image, text, video

INTRODUCTION

The steganography has been used for long time before. The main use for it was for military and government messages, nowadays; the approaches of steganography become widely used for many purposes. Anyway, the researchers provide and found out many approaches while others enhanced the methods and the approaches of the steganography in order to improve the steganographic applications (Othman *et al*., 2009).

Basically, all steganography technique have to satisfy two basic requirements. The first requirements perceptual transparency i.e., cover object and Stego object (object content secret message) (Ahmed *et al*., 2010). In this study a discussion about the existent methods or approaches for the steganography and how the researchers improve it within more than 10 years will be presented.

CRITICAL REVIEW

The critical review will be depended on two manners capacity and security which are the steganography aspects. The first manner concern with the security aspect; Steganography and cryptography are in fact complementary techniques (Naji *et al*., 2009). The process of sharing secure message within insecure channel require authentication and integrity to the data in such a way that even the message has been altered by unauthorised party it is still easy to detect that some changes has been done to the message. The second manner concern with the capacity, there are some techniques facing the capacity limitation problem, in general, the image has limited capacity when use it as a cover medium and it's easier to being tested by the attacker it than the video where the video consist of a set of images and can use more than one image within the video as a carrier cover and more difficult to test it because the sequence of the stego image within the video is unknown by the attacker.

TEXT BASED APPROACHES

The text files have been used for steganography techniques in Table 1, the idea of using the text to hide the secure message or information is to embedding the secure information within the text bits.

Aabed *et al.* (2007) and Gutub and Fattani (2007) proposed an Arabic text steganography method. Gutub and Fattani (2007) proposed steganography approach suitable for Arabic texts. The approach hides secret

Table 1: Text-based steganography

Study	Cover carrier	Security	Method
Aabed *et al.* (2007)	Text	Pure steganography	LSB
Gutub and Fattani (2007)	Text	Pure steganography	LSB

Corresponding Author: Ali K. Hmood, Faculty of Computer Science and Information Technology,
University of Malaya, 50603, Kuala Lumpur, Malaysia

information bits within the letters benefiting from their inherited points. To note the specific letters holding secret bits, the scheme considers the two features, the existence of the points in the letters and the redundant Arabic extension character. The author used the pointed letters with extension to hold the secret bit one and the un-pointed letters with extension to hold zero. While Aabed *et al*. (2007) embedded the secret information into text cover media. This study utilised the advantages of diacritics in Arabic to implement text steganography. Diacritics - or Harakat - in Arabic are used to represent vowel sounds and can be found in many formal and religious documents. The proposed approach uses eight different diacritical symbols in Arabic to hide binary bits in the original cover media. The embedded data are then extracted by reading the diacritics from the document and translating them back to binary. However, both approaches used for text-based steganography which is so limited in capacity and it is the easiest approach to be altered even accidently since it is use the visible text to hide the secure message.

IMAGE BASED APPROACHES

The image is one of the possible cover for the secure message or information in Table 2, also images are the most popular carrier file for steganography because of the abundance of images available on the internet (Al-Azawi and Fadhil, 2010). The using of the image as a cover carrier is the most widely used for steganographic application.

Table 2: Image-based steganography

Study	Cover carrier	Security	Method
Zaidan *et al*. (2009)	Image	Pure steganography	LSB
Zaidan *et al*. (2009)	Image	Pure steganography	LSB
Kim and Kim (2007)	Image	Pure steganography	LSB
Wang *et al*. (2001)	Image	Pure steganography	LSB
Moskowitz *et al*. (2000)	Image	Pure steganography	LSB
Su and Kuo (2003)	Image	Pure steganography	BPCS
Niimi *et al*. (2002)	Image	Pure steganography	BPCS
Spaulding *et al*. (2002)	Image	Pure steganography	BPCS
Hossain *et al*. (2010)	Image	Pure steganography	Four neighbours diagonal neighbours eight neighbours
Wang *et al*. (2008)	Image	Pure steganography	Two consecutive pixels
Lee *et al*. (2008)	Image	Pure steganography	Centralized difference expansion
Fu and Au (2003)	Image	Pure steganography	Conjugate error diffusion
Chang and Tseng (2004)	Image	Pure steganography	Side match vector quantization

Hossain *et al*. (2010) three different steganographic methods for gray level images are presented in this study. Four neighbours, diagonal neighbours and eight neighbours' methods are employed in proposed approach. These methods utilise a pixel's dependency on its neighbourhood and psycho visual redundancy to ascertain the smooth areas and complicated areas in the image. However, the presented method used the image as a cover carrier; even though the capacity improved by the new method but the limitation of image size is still founded. (Zaidan *et al*., 2009; Zaidan and Zaidan, 2009) used the property of human vision system that helps to increase the size of data hidden in the bitmap (bmp) and (JPG) image practically. The presented study discussed the impact of increasing data hidden on the images texture for colour image and gray level image where, quality of image and the quantity of data hidden work in reverse side once the amount of data hidden in the image increased the quality of the image will be affected. The presented study tried to enhance the capacity problem within the image-based steganography using the Least Significant Bit (LSB) while the image steganography is still limited capacity due to the limitation of the image size. While Wang *et al*. (2008) presented a new image steganographic technique using the Least Significant Bits (LSBs). In order to avoid the falling-off-boundary problem the presented method used the pixel-value differencing and the modulus function. The method provided a good quality degradation for the stego-image to become more imperceptible to the human eye by considering that the smoother area is, the less secret data can be hidden; while, the more edges an area has, the more secret data can be embedded. The authors tried to greatly reduce the image distortion caused by the hiding of the secret data. The Peak Signal-to-Noise Ratio (PSNR) is the used metric to measure the quality of the proposed approach; the author depend on this metric in order to show the enhancement of their approach to hide secret message into image, while this metric is not reliable to give a dependable results as we will discuss later.

Lee *et al*. (2008) presented an adaptive lossless data hiding method which is capable of offering greater embedding capacity than the existing methods, by utilizing a block-based lossless data embedding algorithm where the quantity of the hidden information each block bears is variable. The presented method used centralised difference expansion, which is an improved version of generalised difference expansion where the distortion of the stego-image is reduced. The payload of each block depends on its cover image complexity in order to reduce

the image distortion and increase the hiding capacity (Lee *et al*., 2008). However, the proposed method in this study calculated the Peak Signal-to-Noise Ratio (PSNR) and compared it with other studies results of the PSNR to show that their approach is better than others, while the PSNR is not reliable metric for the image quality and is not dependable for the steganographic object in order to show the security of the stego-image. While Kim *et al*. (2007) proposed an efficient algorithm for information hiding in the Least Significant Bits (LSBs) of JPEG coefficients, the proposed method uses modified matrix encoding to choose the coefficients whose modifications introduce minimal embedding distortion (Kim *et al*., 2007). However, the author focusing on enhancing the image quality to reduce the distortion being added to the image, while the steganography is not concern with the distortion only, yes it's an important factor in steganography but the security aspects is the goal of steganography. Chang and Tseng (2004) proposed side match scheme to hide the secret message into image as a carrier cover. The method exploits the correlation between neighbouring pixels to estimate the degree of smoothness or contrast of pixels. If the pixel is located in edge area, then it may tolerate larger changes than those in smooth areas. The two-sided, three-sided and four-sided side match methods are employed in this approach. Niimi *et al*. (2002) and Spaulding *et al*. (2002) use image as the cover medium for the secure message while the Bit-Plan Complexity Segmentation (BPCS) used for embedding the secure message. Spaulding *et al*. (2002) proposed a Bit-Plan Complexity Segmentation (BPCS) for lossy compressed image. The proposed approach does not achieved a high capacity as it achieved embedding rates of around 25% of the compressed image size were achieved with noticeable degradation in image. However, other studies achieved around 50% of the image size without compression and with a small degradation. While Niimi *et al*. (2002) used the Bit-Plan Complexity Structure (BPCS) to hide the secure message within the cover carrier. The BPCS-Steganography to palette-based images which consists of a palette storing colour vector information and an index image whose pixel value is corresponding to an index in the palette is used to apply the steganography techniques into image. However, the two studies are suffering from the capacity limitation due to the image size limitation, as well as the steganography approaches cannot ensure the security of the shared message which led to the compulsory integration between the steganography technique with others such as cryptography to achieve a better security level.

While Su and Kuo (2003) a steganographic scheme to hide a large volume of data into JPEG2000 compressed images has been proposed. The authors said that the encryption is not applicable in their approach since the approach cannot guarantee that the hidden information can be transmitted without errors due to the truncation of JPEG2000. Beside, the capacity problem within the image based steganography. As well as the compression can affect the quality of the image directly.

Fu and Au (2003) proposed data hiding using conjugate error diffusion to hide an invisible binary visual pattern in two or more error diffused halftone images, the proposed method added the distortions of limited to the multi-tone image such that the pixel values of the various halftone images tend to be conjugate to each other. With the conjugate relationship, the dark regions of the hidden pattern would appear on the halftone images when they are overlaid. The secret sharing requirement was not found in this study while there is no authentication technique and no robustness. In additional, the image-based steganography is facing the capacity and easy to detect problems.

While in Moskowitz *et al*. (2000) proposed a new paradigm hidden in steganography, the authors worked on greyscale images with dimensions 500×500 pixels, the authors mentioned that the new method is strong for hidden the message inside images but not robust method. The new method has replaced the two Least Significant Bits (LSB) of the pixel with the matching two bit section, the new method has limited for the text length it was 249 (ASCII) characters only. The text end with null character, this way can help the user to send a message shorter than 249 characters (Shirali-Shahreza *et al*., 2008). To extract the embedded text, the method is reversed. When the reverse algorithm reads the null character, it stops the extraction process. The authors has discussed why the steganography suffer from fail in some methods and the authors found that the fail come from adding noise during the steganographic embedding phase. The capacity of this approach is limited as it is become not useful for sharing secure message using steganography technique.

While Wang *et al*. (2001) developed a method to embed important data in the host image so that the interceptors will not notice about the existence of the data using Least Significant Bits (LSBs) substitution, develop a genetic algorithm to solve the problem of hiding important data in the rightmost LSBs of the host image. The author used the Peak Signal-to-Noise Ratio (PSNR) to demonstrate the result while the PSNR is insufficient metric for such systems.

Table 3: Image-based steganography and cryptography

Study	Cover carrier	Security	Method
Fridrich *et al.* (2005)	Image	Robust	Perturbed quantization
Solanki *et al.* (2006)	Image	Robust	Quantizationindex modulation with dithering
Potdar *et al.* (2005)	Image	Robust	Not specified
Franz and Schneidewind (2004)	Image	Stego-key	ConDith
Chang *et al.* (2002)	Image	Cryptography and steganography	Least two Significant bits (LTSBs)
Venkatraman *et al.* (2004)	Image	Cryptography and steganography	LSB
Wang (2005)	Image	Cryptography and steganography	Modulus operations

However, within all the earlier studies the authors have been used pure steganography approaches, they tried to enhance the steganography aspects but without ensuring the security of the steganographic object. The secure channel can be used to securely transfer message or information between two parties. The integrity and/or authentication can be achieved over an insecure channel by cryptosystems. Since no technique of hiding information can ensure perfect secrecy (Venkatraman *et al*., 2004). However, by combining steganography with other techniques, such as cryptography, a higher chance of success can be achieved (Naji *et al*., 2009). In Table 3, the cryptography and steganography has been used together to enhance the security aspects.

For secure message sharing, Fridrich *et al*. (2005) proposed a wet study codes and passive-warden approach for steganography called perturbed quantization. In this method the non-quantized values of the processed cover object are considered as side information to confine the embedding changes to those non-quantized elements whose values are close to the middle of quantization intervals, while the lossy compression for the image are employed in this method. The choice of the selection channel calls for wet study codes as they enable communication with non-shared selection channel (Fridrich *et al*., 2005). However, the author used the image compression which is directly affecting the perceptual quality of the image and makes it suspicious.

Other technique for the security aspects, Solanki *et al*. (2006) presented the new design of steganographic method that can provide provable security by achieving zero Kullback Leibler divergence between the cover and the stego signal distributions, while hiding at high rates. The approach was aim to reserve a number of host symbols for statistical restoration. A dynamic embedding approach called Quantisation Index Modulation together with dithering approach. The proposed method avoids hiding in low probability regions of the host distribution. However, the cryptography combined with steganography in this method. But the usage of image based steganography suffering from the capacity limitation.

Wang (2005) proposed a modulo operator for embedding secret image, the authors proposed a novel mechanism using modulus operations to incorporate secret data (with image form) into a host-image. The authors proposed two kinds of secret images where the capacities of these two types are half the size and a quarter the size of the chosen host-image, while not only can the secret images be totally embedded, but the extra information, such as the auxiliary table, assisting the secret extraction is released as well. However, the authors approve their method by measuring the quality of the stego-image using PSNR metric, which is unreliable for such measurement.

Potdar *et al*. (2005) presented a fingerprinted secret sharing steganography for robustness against image cropping attacks, the presented method tried to break the main secret into multiple parts and hide them individually in a cover medium. The proposed approach used to compress the data to a considerable extent and for recover the shared secret, the authors used Lagrange Interpolating Polynomial method. The embedding can be done using any steganographic algorithm. The proposed method used the image cropping to offer robust mechanism to protect data loss. The image based steganography is still suffered from the capacity requirement; as the capacity is one of the main aspects of steganography as well as the authentication is not satisfied by this approach (Potdar *et al*., 2005).

The hiding information techniques lack of assuring the message security. However, a combination between steganography with cryptography, a higher chance of success can be achieved (Venkatraman *et al*., 2004). Due to this reason, Venkatraman *et al*. (2004) proposed a significance of steganography on data security, the new method attempted to bring out the significance of the steganographic techniques that are employed in information processing algorithms for data security. The study suggested how a variation of the LSB insertion algorithm can be used for achieving better security and also improved covertness. The authors found out the results of steganalysis can be used to change or improve embedding techniques. However, the author has focusing on image based steganography only, the author tried to cover some aspects of steganography but the limitation of capacity has not overcame.

Franz and Schneidewind (2004) proposed an adaptive dithering based steganography, the authors suggested the use of white noise dithering to develop adaptive steganographic algorithms, as well as drawing out possibilities to exploit the classification provided by dithering for embedding and develop two basic algorithms: Adaptive Selection (AdSel) and Adaptive Modification (AdMod). Since the original dither criterion is not sufficient for steganography, the author modified the existent dither criterion and developed ConDith as an algorithm that is based on AdSel. The authors investigated further improvements of this algorithm ConDithSpread, ConDithInc and ConDithNoise. The authors claim in the proposed study there are extensive tests confirmed the achieved improvements (Franz and Schneidewind, 2004). However, the authors used a steganographic key which is generated to specify the selected bits for hiding the message instead of using the cryptography techniques. The stego-key is not really reliable for security aspects since it has not the ability to prevent message disclosing.

Chang *et al*. (2002) used the image based steganography conjunction with cryptography. The proposed method modifies the quantization table first. Next, the secret message is hidden in the cover-image with its middle-frequency of the quantized DCT coefficients modified. Finally, a JPEG stego-image is generated. The authors compare their method with other to show their enhancements they rely on PSNR metric which is not reliable in measuring such systems.

All the above presented studies are used the image based steganography approaches in conjunction with cryptography, but the size is still the problem with these approaches. Since there is a limitation on how much information can be hidden into an image (Chang *et al*., 2002), making difficult to use the image methods, then in order to help to increase collaborative documents security. The video based steganography has been found to overcome the capacity problem, the video consist of a number of images placed in a frames to be presented in sequence one after the others. We can use any image within the video to hide the secure message with it, the use of video based steganography has another advantage as the discloser will facing a problem to attack the image since the sequence of the image within the video is unknown for the attacker, so the attacker need to check all the images within the video which make it more difficult to attack the secure message. As well as the video-based steganography has the lowest chances of being suspicious because of the quickly displaying of the frames so it's become harder to be suspected by the human vision system.

VIDEO BASED APPROACHES

The video is consisting of a number of still image separated in frames where it is possible to hide in all the frames to increase the capacity. In Table 4, video based steganography has been proposed.

The capacity problems overcame by Noda *et al*. (2004) the proposed method was based on wavelet compression for video data and Bit-Plane Complexity Segmentation (BPCS) steganography. The author enhanced the capacity problems by using the video-based steganography. However, the secret sharing requirements has not appeared in this study. The hash code or digital signature is the widely used techniques for integrity and authentication issues, when the steganography combined with these techniques a highly secure secret sharing system can be proposed. As well as the compression can affect the quality of the video and is make it suspicious to the attacker. A video error correction using steganography has been proposed by (Robie and Mersereau 2002) since the transmission of any data is always subject to corruption due to errors, then the video transmission (because of its real time nature) must deal with these errors without retransmission of the corrupted data. However, the study proposed another application for the steganography rather than for security purposes. On another hand, Jalab *et al*. (2009) proposed collaborate approach for select frame using Bit Plane Complexity Segmentation (BPCS) for hiding data within MPEG Video. The proposed approach invented a high secure data hidden using select frame from MPEG Video. However, the proposed approach achieved a high capacity using video as a cover carrier but the steganography alone unable to achieve high secure system for message sharing purposes. Eltahir *et al*. (2009) proposed approach for video steganography using the Least Significant Bits (LSBs). The method considered the digital video file as separated frames and changed the output image displayed on each video frame by hidden

Table 4: Video-based steganography

Study	Cover carrier	Security	Method
Noda *et al*. (2004)	Video	Pure steganography	BPCS
Jalab *et al*. (2009)	Video	Pure steganography	BPCS
Robie and Mersereau (2002)	Video	Pure steganography	Discrete cosine transformation
Eltahir *et al*. (2009)	Video	Pure steganography	LSB
Bhaumik *et al*. (2009)	Video	Pure steganography	LSB
Wu *et al*. (2003)	Video	Pure steganography	Modulation and multiplexing

data that does not visually change the image. With this technique, one can apply hidden information with more space better than other steganography media. However, the authors used the video-based steganography to enhance the capacity of the hidden message but the security requirements such as data integrity has not appeared in the study (Eltahir *et al*., 2009).

While Bhaumik *et al*. (2009) suggested another video-based steganography. By using AVI videos which are large in size but still can be transmitted from source to target over network after processing the source video by using the data hiding and extraction procedure securely. There are two different procedures, which are used in this study at the sender and receiver sides respectively. The procedures are used as the key of data hiding and extraction processes. However, the suggested key in this study does not meet the security standards and it is unable to ensure the authentication and integrity of the data or the message.

Wu *et al*. (2003) applied multilevel embedding to allow the amount of embedded information that can be reliably extracted to be adaptive with respect to the actual noise conditions. The authors proposed strategies for handling different embedding capacity from region to region within a frame as well as from frame to frame. The authors also embed control information within the video to facilitate the accurate extraction of the user data payload and to combat such distortions.

However, within all the earlier presented studies the authors has used the video-based steganography as a medium carrier, but the security requirements does not satisfied in those study. The security for the message sharing purpose required the integrity and authentication for the message to be achieved and tested in order to ensure that the data came from the authorised sender and it has not been altered by unauthorised parties during the transmission using insecure channel. In Table 5, the cryptography and video based steganography has been used together to enhance the security aspects.

The enhancements of the security in steganography approaches can be achieved by integrate the steganography with other techniques. In Chae and Manjunath (1999) proposed a video-based steganography in which the embedded signature data is extracted without knowing the original host video. The proposed method enables high rate of data embedding. Embedding is based on texture masking and utilizes a multi-dimensional lattice structure for encoding signature information. Signature data is embedded in individual video frames using the block DCT. However, the author claim that this approach is robust for motion compensated codes, such as MPEG-2, without showing the proof for the robustness.

Table 5: Video-based steganography and cryptography

Study	Cover carrier	Security	Method
Chae and Manjunath (1999)	Video	Robust	Multidimensional lattices
Socek *et al*. (2007)	Video	Cryptography and steganography	Permutation-based transformations
Westfeld and Wolf (1998)	Video	Cryptography and Steganography	LSB
Liu *et al*. (2008)	Video	Cryptography and steganography	Least value DCT coefficients
Zaidan and Zaidan (2009)	Video	Cryptography and steganography	LSB

While Socek *et al*. (2007) proposed video encryption algorithm designed for both lossless and lossy low-motion spatial-only video codec. The proposed encryption method can thus be performed before compression at the encoder side and after decompression at the decoder side. As well the author introduced a new type of steganography as an extension to the encryption approach. The proposed steganographic scheme enables disguising a video with another video, which is a new concept in video-based steganography. However, the encryptions usually increase the size of the cipher-text which is affecting the capacity of the secret message.

On the other hand, Westfeld and Wolf (1998) presented the steganography in a video conferencing, the video conference used for the implementation of the steganographic system presented in this study works on the H.261 standard. However, the H.261 is not adequate to be used on the Internet, where just low bit-rate is available (De Oliveira, 1997).

While Zaidan and Zaidan (2009) proposed a collaborate approach between steganography and cryptography. The approach provided a high secure data hidden using Public Key Infrastructure (PKI) method. However, the security aspect has been considered in this study, although the size of the cipher-text is a genuine problem for steganography. Furthermore, PKI encryption has been proposed for the purpose of integrity. A solution of using hash function instead of PKI can give faster processing, less size for authentication of the message.

The use of video as a carrier cover for the secure message is overcame the capacity problem and added small enhancement to the security aspects. The integration of steganography and cryptography techniques provided powerful systems for sharing secure messages. This integration especially within video cover carrier is a good stage of such systems, but the capacity of the produced message from the cryptography technique which is called cipher-text is larger than the original message (plaintext). The cryptography techniques

increase the size of message after the encryption to be greater than the size of the original message (Shin and Choi, 2009), on another hand (Biham, 1991) shown that the cipher-text size is much larger than the plaintext size by using the cryptography techniques. While Wong *et al.* (2005) found out the cipher-text size is usually long, at least twice that of the original plaintext. In additional, some specific implementations of cryptography required special hardware at appreciable costs (Perritt, 1994) as well as the cryptographic functions require considerable computation and CPU processing time, which might introduces the binding latency (Kim and Han, 2006; Kim *et al.*, 2007). All these led to make the use of the hash function as one type of cryptography more feasible, the main goal of using the hash code is to ensure data integrity and authentication which considered the main aspects of sharing secret message within insecure channel.

CONCLUSIONS

The review has shown above presents the steganography approaches and how some researchers tried to enhance the limitation of steganography. Before 10 years the capacity of the secure image was limited (Moskowitz *et al.*, 2000) while now some researchers provide new approaches which can embed secure message or image within more than 50% of the original image size. As we shown in the earlier study on steganography there are many use for the steganography even not for pure security where sometimes it is usable for error correction like by Robie and Mersereau (2002). For the capacity purpose there is a limitation on how much information can be hidden into an image, making difficult to use the image methods (Chang *et al.*, 2002). In the video steganography we have a flexibility of make a selective frame steganography to higher the security of the system or using the whole video for hiding a huge amount of data (Zaidan and Zaidan, 2009). That reason makes the use of video-based steganography more eligible. As well as, the confidentiality need to be tested through testing the quality of steganographic object. In addition, the current metrics which is used for measuring quality of steganographic objects are not sufficient for this kind of test.

In the other hand, for the highly secure applications there are some users need special quality characteristics or security requirements such as integrity and authentication. The authentication technique allows the receiver to be certain that a message is genuine, or in another words, the message generated by the original sender. According to Preneel and van Oorschot (1995), Haber and Kamat (2006), Sun *et al.* (2008) and Alghathbar (2010), information that is transmitted or stored in insecure channels is needed to be checked to assure its reliability. While integrity is for assuring the receiver of the message that the received message is exactly what the sender transmitted and there are no intentional or accidental changes has been done by unauthorised part. The integrity usually comes in conjunction with authentication techniques (IETF, 1999; Aura *et al.*, 2000; Haber and Kamat, 2006; Alghathbar, 2010). By using the authentication techniques, the attacker even one with infinite computer resources cannot forge or modify a message without detection (Wegman and Carter, 1981). The user needs for trusted system in order to do a secure transformation for data or information.

ACKNOWLEDGMENTS

This study has been funded by the University of Malaya, under the Grant No. (P0033/2010A). The author would like to take this opportunity to thank and acknowledge his supervisors: Dr. Hamid Jalab and Dr. Zarinah Mohd Kasirun, for having rendered their ceaseless and unconditional support throughout the entire duration of the study. The author would also like to extend his heartfelt gratitude to all his friends and associates who had offered him the much needed assistance and encouragement from the start to the end of the research period.

REFERENCES

Aabed, M.A., S.M. Awaideh, A.M. Elshafei and A.A. Gutub, 2007. Arabic diacritics based steganography. Proceedings of the International Conference on Signal Processing and Communications, Nov. 24-27, Dubai, UAE, pp: 756-759.

Ahmed, M.A., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2010. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Applied Sci., 10: 59-64.

Al-Azawi. A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Alghathbar, K., 2010. Code based hashing technique for message authentication algorithms. J. Inform. Assurance Security, 5: 9-20.

Aura, T., P. Nikander and J. Leiwo, 2000. DOS-Resistant Authentication with Client Puzzles. Springer, New York.

Bhaumik, A.K., M. Choi, R.J. Robles and M.O. Balitanas, 2009. Data hiding in video. Int. J. Database Theory Appl., 2: 9-16.

Biham, E., 1991. Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at Eurocrypt'91. Springer, New York.

Chae, J.J. and B.S. Manjunath, 1999. Data hiding in video. Proceedings of the 6th IEEE International Conference on Image Processing, Oct. 1999, IEEE, pp: 243-246.

Chang, C.C., T.S. Chen and L.Z. Cheng, 2002. A steganographic method based upon JPEG and quantization table modification. Inform. Sci., 141: 123-138.

Chang, C.C. and H.W. Tseng, 2004. Steganographic method for digital images using side match. Pattern Recognition Lett., 25: 1431-1437.

De Oliveira, J., 1997. A Java H. 263 decoder implementation. Electrical and Computer Engineering Department, University of Ottawa. http://www.lncc.br/~jauvane/papers/H263JavaDecoder.pdf.

Eltahir, M.E., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2009. High rate video streaming steganography. Proceedings of the 2009 International Conference on Future Computer and Communication, April 03-05, IEEE Computer Society, Kuala Lumpur, Malaysia, pp: 550-553.

Franz, E. and A. Schneidewind, 2004. Adaptive steganography based on dithering. Proceedings of the 2004 Workshop on Multimedia and Security, Sept. 20-21, ACM, New York, USA., pp: 56-62.

Fridrich, J., M. Goljan and D. Soukal, 2005. Perturbed quantization steganography. Multimedia Syst., 11: 98-107.

Fu, M.S. and O.C. Au, 2003. Steganography in halftone images: conjugate error diffusion. Signal Process., 83: 2171-2178.

Gutub, A.A.A. and M.M. Fattani, 2007. A novel Arabic text steganography method using letter points and extensions. World Acad. Sci. Eng. Technol., 27: 28-31.

Haber, S. and P. Kamat, 2006. A content integrity service for long-term digital archives. Proceedings of the Archiving 2006 Conference, May 23-26, Ottawa, Canada, pp: 6-6.

Hossain, M., S. Al Haque and F. Sharmin, 2010. Variable rate steganography in gray scale digital images using neighborhood pixel information. Int. Arab J. Inform. Technol., 7: 34-38.

IETF, 1999. PPP EAP TLS authentication protocol. RFC 2716 15. http://www.ietf.org/rfc/rfc2716.txt.

Jalab, H., A. Zaidan and B.B. Zaidan, 2009. Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation. J. Comput., 1: 108-113.

Kim, P. and J. Han, 2006. New authorizing binding to reduce binding latency during mobile ipv6 handover procedure. IJCSNS, 6: 1-7.

Kim, P.S. and Y.J. Kim, 2007. A new mechanism for recognizing handover situation in vertical handovers. Proceedings of the 6th IASTED International Conference on Communications, Internet and Information Technology, July 02-04, ACTA Press, Anaheim, CA, USA., pp: 185-188.

Kim, Y., Z. Duric and D. Richards, 2007. Modified Matrix Encoding Technique for Minimal Distortion Steganography. In: Lecture Notes in Computer Science, Camenisch, J. *et al.* (Eds.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-74123-7, pp: 314-327.

Lee, C.C., H.C. Wu, C.S. Tsai and Y.P. Chu, 2008. Adaptive lossless steganographic scheme with centralized difference expansion. Pattern Recognition, 41: 2097-2106.

Liu, B., F. Liu, C. Yang and Y. Sun, 2008. Secure steganography in compressed video bitstreams. Proceedongs of the 3rd International Conference on Availability, Reliability and Security, March 4-7, IEEE, pp: 1382-1387.

Moskowitz, I.S., G.E. Longdon and L. Chang, 2000. A new paradigm hidden in steganography. Proceedings of the 2000 Workshop on New Security Paradigms, Sept. 12-22, ACM, Ballycotton, County Cork, Ireland, New York, pp: 41-50.

Naji, A.W., A.A. Zaidan and B.B. Zaidan, 2009. Challenges of hidden data in the unused area two within executable files. J. Comput. Sci., 5: 890-897.

Niimi, M., H. Noda and E. Kawaguchi, 2002. High capacity and secure digital steganography to palette-based images. Proceedings of the International Conference on Image Processing, Sept. 22-25, IEEE, pp: 917-920.

Noda, H., T. Furuta, M. Niimi and E. Kawaguchi, 2004. Application of BPCS steganography to wavelet compressed video. Proc. Int. Conf. Image Process., 4: 2147-2150.

Othman, F.,L. Maktom, A.Y. Taqa, B.B. Zaidan, A.A. Zaidan, 2009. An extensive empirical study for the impact of increasing data hidden on the images texture. Proceedings of the 2009 International Conference on Future Computer and Communication, April 3-5, IEEE Computer Society, Kuala Lumpur, Malysia, pp: 477-481.

Perritt, H.Jr., 1994. Permission headers and contract law. IMA Intellectual Property Project Proc., 1: 27-48.

Potdar, V. M., S. Han and E. Chang, 2005. Fingerpnnted secret sharing steganography for robustness against image cropping attacks. Proceedings of the 3rd IEEE International Conference on Industrial Informatics, Aug. 10-12, IEEE, Perth, Australia, pp: 717-724.

Preneel, B. and P. van Oorschot, 1995. MDx-MAC and building fast MACs from hash functions. Proceedings of the Advances in Cryptology, Aug. 1995, Springer-Verlag, pp: 1-14.

Robie, D.L. and R.M. Mersereau, 2002. Video error correction using steganography. EURASIP J. Applied Signal Process., 2002: 164-173.

Shin, K. and H. Choi, 2009. A self-certified signcryption scheme for mobile communications. Proceedings of the USENIX Security Symposium '09 (USENIX Security), Aug. 10-14, Montreal, Canada, pp: 12-17.

Shirali-Shahreza, M. and S. Shirali-Shahreza, 2008. High capacity persian/arabic text steganography. J. Applied Sci., 8: 4173-4179.

Socek, D., H. Kalva, S.S. Magliveras, O. Marques, D. Culibrk and B. Furht, 2007. New approaches to encryption and steganography for digital videos. Multimed. Syst., 13: 191-204.

Solanki, K., K. Sullivan, U. Madhow, B.S. Manjunath and S. Chandrasekaram, 2006. Provably secure steganography: Achieving zero k-l divergence using statistical restoration. Proceedings of the IEEE International Conference on Image Processing, (ICIP'06), USA., pp: 1-4.

Spaulding, J., H. Noda, M.N. Shirazi and E. Kawaguchi, 2002. BPCS steganography using EZW lossy compressed images. Pattern Recognition Lett., 23: 1579-1587.

Su, P.C. and C.C. J. Kuo, 2003. Steganography in JPEG2000 compressed images. IEEE Trans. Consumer Electronics, 49: 824-832.

Sun, Q., J. Apostolopoulos, C.W. Chen and S.F. Chang, 2008. Quality-optimized and secure end-to-end authentication for media delivery. Proc. IEEE., 96: 97-111.

Venkatraman, S., A. Abraham and M. Paprzycki, 2004. Significance of steganography on data security. Int. Conf. Inform. Technol., 2: 347-351.

Wang, R., C. Lin and J.C. Lin, 2001. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition, 34: 671-683.

Wang, S.J., 2005. Steganography of capacity required using modulo operator for embedding secret image. Applied Math. Computation, 164: 99-116.

Wang, C.M., N.I. Wu, C.S. Tsai and M.S. Hwang, 2008. A high quality steganographic method with pixel-value differencing and modulus function. J. Syst. Software, 81: 150-158.

Wegman, M. and J. Carter, 1981. New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci., 22: 265-279.

Westfeld, A. and G. Wolf, 1998. Steganography in a Video Conferencing System. Springer, New York.

Wong, K., K. Man, S. Li and X. Liao, 2005. A more secure chaotic cryptographic scheme based on the dynamic look-up table. Circuits Syst. Signal Process., 24: 571-584.

Wu, M., H. Yu and B. Liu, 2003. Data hiding in image and video: part II-designs and applications. IEEE Trans. Image Process., 12: 696-705.

Zaidan, A. and B. Zaidan, 2009. Novel approach for high secure data hidden in MPEG video using public key infrastructure. Int. J. Comput. Network Security, 1: 1985-1553.

Zaidan, B., A.A. Zaidan, F. Othman, R.Z. Raji, S. Mohammed and M. Abdulrazzaq, 2009. Quality of image vs. quantity of data hidden in the image. Proceedings of the 2009 International Conference on Image Processing, Computer Vision and Pattern Recognition, (ICIPCVPR'09), CSREA Press, Las Vegas Nevada, USA., pp: 343-350.