Journal of Computer Science

Original Research Paper

Efficient Multi-Secret Digital Images Steganography

Haval Muhammed Sidqi

Department of Database, Institute of Computer, University of Sulaimani Polytechnic, KRG, Iraq

Article history
Received: 16-10-2019
Revised: 13-02-2020
Accepted: 21-02-2020

E-mail: haval.sidqi@spu.edu.iq

Abstract: The new conceptions of more than one secret message and false digital image steganography are presented in the current paper. One of the major ideas in these approaches is embodiment of more than one message in one container (digital image). The secrets that are hidden are known as real and false messages. The former one includes basic data that should be transferred between various parties in a secure manner. The second one is a bait for in order to focus attention on a non-important message. When it is discovered that there exists the actual information, this false and multiple data hidden steganography is cracked, regardless of detection of false message. Many various applications can be found for these concepts, particularly in situations that there is close monitoring over the communication channel between a receiver and a sender and there is suspicion of using steganography. In this case, probably the transferred data would be examined in detailed. The concepts that are defined in the current paper would be helpful for overcoming this problem through ignoring an invented message and thus, deception of the warden. It can be perceived as an additional benefit that it is possible to send both false and real data at the same time. The presented idea actually gives the opportunity of the establishment of a subliminal channel during the transfer of hidden information by the use of digital images.

Keywords: Cryptographic Protocols, Information Splitting, Information Hiding, Steganography

Introduction

Steganography is the term used for describing an approach of hiding data so that discovery of secret data by unplanned receivers is prevented (Bailey and Curran, 2005). The steganography is successfully used when the presence of the secret message is not detected; otherwise, it will be broken. Therefore, one of the major dimensions of any steganographic approach is the provision of the high level of detectability (Budhia *et al*., 2006). Container modification is the famous way of digital steganography in which is changed in hiding operation and it is sent to the receiver for data extraction. The challenge is that the container's changes alters its statistics (for example, histogram). In the case that warden has accessibility to carrier, he would attempt to verify it for the presence of the secret message. Steganalysis means the actions that warden takes for finding hidden data and mostly it is on the basis of the statistical distribution (Castiglione *et al*., 2007).

The embedded data length influences the number of alterations that are made to container and, thus, the detection likelihood. Hence, undetectability and capacity are the requirements that compete (Castiglione *et al*., 2012) and achieving an acceptable level of both is a challenge in steganography. An appropriate carrier selection is an essential issue that influences the security of system. The most prevalent digital containers include network packets, images, text, video and audio files due to their extensive use in network communication (Castiglione *et al*., 2011a).

Nevertheless, there have also been some proposals for using various media for steganography including electronic mail messages, documents (Castiglione *et al*., 2011b) and social networks. A human brain is not able to distinguish some sounds and colors and they are seen as identical. It can be used for concealing some information such as in images.

More than One Secret Message and False Steganography

Targeted or blind steganalysis algorithms may detect these alterations (Castiglione *et al*., 2011c). For this reason, the focus of many steganographic approaches is on minimization of embedding impact.

In the suggested method, some changes intentionally are made on carrier for increasing undetectability of some data for others:

- Real message (as the main secret information) that is required to be sent discreetly to receiver from sender
- Additional message (false) information, which are immaterial for covert communication goals at deceiving adversary (illegitimate parties that might oversee the communication channel)

Both types of messages, i.e., false and real messages, are included into one container (Fig. 1). It is possible to use any steganography approach, but it is assumed that discovery of the real message is more difficult than the false message. In cases that one secret data is embedded, there are larger modifications but the presence of the false secret data, the detection of which is easier, distracts attention from the real message. If the false secret hidden information is detected, the warden is probably persuaded that the secret communication is discovered and searching would not be continued:

1. Not detection of all messages-successful false steganography
2. Detection of false message, but real message stays secret-successful false steganography
3. Detection of real message-broken false steganography; non-importance of false message detection (Lahrod *et al*., 2016)

These three possible situations are related to detection of data by the warden. The key required for extraction of the real message. Having knowledge of obtaining false secret is probable, but it is not a necessity for the real user since it is not required for covert communication. Disclosing the false secret data is acceptable since its purpose is misinforming adversary through altering the container's statistics. From the steganalyst perspective, modifications of carrier are made when there is hidden data. Applying the rule that the real message detection is more difficult compared to detection of the false secret data, it is probable that just false data will be discovered and real message will remain unseen. It is actually nature of false steganography. The real message can also be hidden in a container and it can be used as subsequent message and it can be embedded in other container. This method can be treated as multi-level steganography (Zhi-Liang *et al*., 2011) in which the real message is hidden on the last level. The most salient difference between two concepts is that the extraction of messages is required on all levels in multi-level steganography in order to achieve secret message. The two ideas can be used together though it worth noting that the present capacity is limited by every level.

The presented approaches are indicated in Fig. 2 and 3. When secret data existence is detected, this concept does not protect against the situation and, consequently, the communication will be blocked by the warden. Nevertheless, it should be mentioned that it is not also done in steganography. The false secret data detection provides adversary data that covert communication occurs. It can be perceived as a disadvantage, but it can be used for benefits. False secret data can be presented both for focusing attention and intentionally giving incorrect information to the warden in case of detection (Ansari *et al*., 2012).

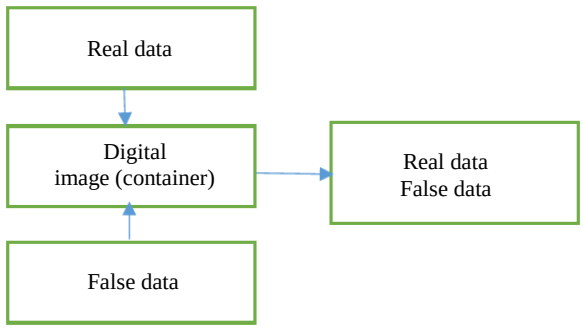


Fig. 1: Shows multi-secret steganography

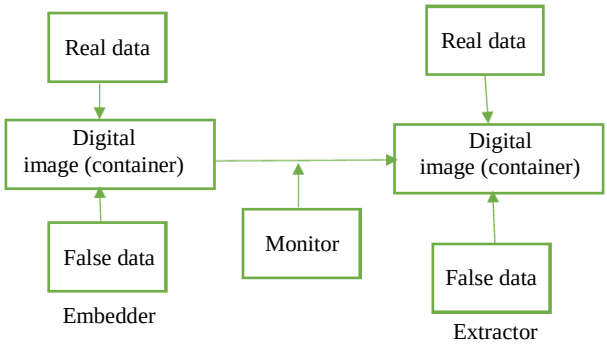


Fig. 2: General idea

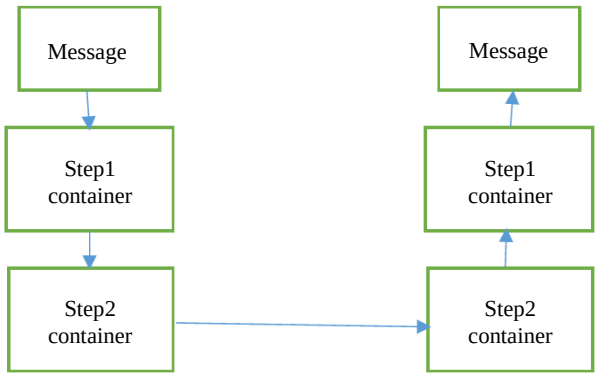


Fig. 3: Multi-level steganography

Applications

It is possible to use the given idea with any steganographic approach. The focus of the current paper is on image steganography. Some experiments made with various algorithms are described below.

The original information will be inserted in the second LSB but for instance, just in a red and blue component.

This choice was made since the sensitivity of the human eye to green is higher than other hues (Tang *et al*., 2016). Consequently, the maximum capacity is decreased, but the real message's undetectability increases. Undetectability can be much improved by appropriate selection of carrier. Mostly green images, e.g., leaves or forest, are a logical selection.

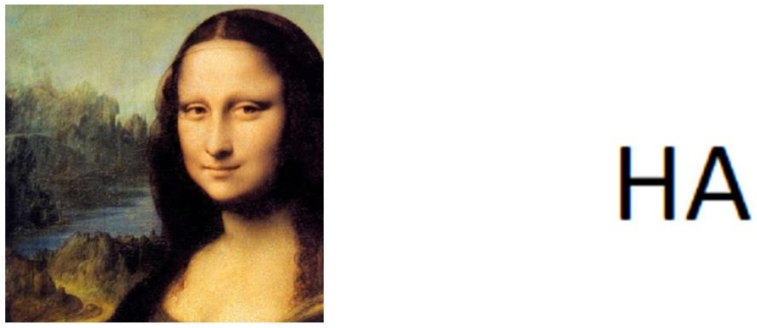
The real message embedding steps are described in the following. Firstly, for the creation of permutation of pixel in dices, a secret key is utilized. This stage intends to spread alterations across the image for avoiding concentration of modifications in one part of the carrier file that can be observed mostly in the case that the secret message's length is shorter than the capacity of the container. P_i means a *i*- the alternative element. A secret information with length of n is embedded in pixels placed at positions p_0,,,,,,,,,,,p_{n-1}. The blue or red component is selected depending on p_i parity. Then, *i* message bit replaces the second LSB of the chosen component of the actual pixel. For extraction of the original information, the receiver is required to compute permutation from the same key for finding altered coefficient values of pixels and it should read second LSB of the correct pixel component. The secret key is share between the receiver and the sender, or it can be hidden steganographically in the container. In this study the false message is utilized as a secret key and RSA algorithm. LSB contains false message, so no collision is observed between extracting and embedding algorithm when they work on different data. The selected secrets are digital images shown in Fig. 4 that before hiding they were encrypted with Rijndael-256. Figure 5 illustrations clean container and the result of embedding original, false and both types of information using the mentioned method. As a result of the encryption, the probabilities of occurrence as 1 and 0 is equal in output data (Norouzi and Mirzakuchaki, 2016). When the inserting is happening, false and real secret information cause disruptions in the container but in a different way Fig. 5. As stated before, LSB technique is used for hiding the false message that is regarded not so secure due to distinctive artifacts developed in the histogram. Investigations on this approach indicate that adjacent bars (that are different only at the least significant bit position) are equalized because of embedding (Dianconu, 2016). These abnormalities normally are not observed in digital images that results in a clear conclusion on the secret data presence. The histogram shape shows the LSB approach. Hence, it is possible that the false information can be shown within steganalysis. It indicates how an illegitimate user is able to take the image from Fig. 4b. The false secret was encrypted in the given example that may suggest the importance of the hidden information. From the perspective of the attacker, the secret was detected, but it might be observed as a false-positive error for the participants.

In addition, different steganographic approaches can be used and hide false and real message in various ways. JPEG steganography is a good example in which:

- It is possible to embed real message in the frequency domain
- It is possible to hide false message in file header

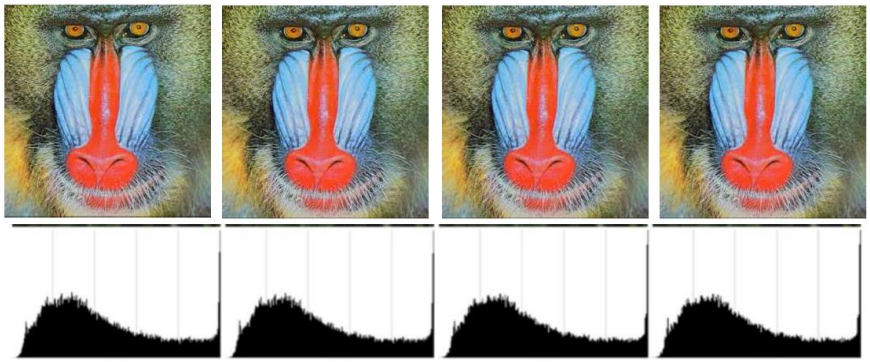
The JPEG file format (Li *et al*., 2016) is keeping lossy compressed data of the image. The file header is segmented and every segment initiates with a pair of bytes (marker). First byte of indicator always is 255 and the second might be different that is used for distinction. Comment is one type of segments, which is identified by marker 254. It might include data regarding quality and program utilized for creating image. The length of the structure and content is not defined; thus, it is possible to use it for embedding some data. Hence, the false information is put in the header's comment segment. Information of the Image are kept as quantized frequency coefficients. Encoding is done as follows. Image is divided into 8×8 pixel squares In the first step. Every piece is then sent to the frequency domain with a discrete cosine transform. In the following step, quantization is done that leads to rounding coefficients and, consequently, some information is lost. The resulting values are structured in a zigzag order causing the concentration of zeros at the stream's end. In the last step, coding of data is done for compressing redundant data. Using F5 algorithm, the real message is hidden in JPEG image (Liu *et al*., 2016). After the quantization of coefficients, the embedding process is done. Firstly, there is a calculated permutation that utilizes a strong random number generator on the basis of a secret key.

The per mutative straddling is intended to scatter modifications uniformly over the whole image. The message is then hidden in nonzero coefficients using matrix encoding. This approaches helps improvement of the embedding efficiency and, consequently, decreases the number of required alterations. The parameters of matrix encoding are associated with the carrier medium capacity as well as the message length. Following these steps, the JPEG compression is continued.



(a) (b)

Fig. 4: Secret images. A. Real secret, B. false secrets



(a) (b) (c) (d)

Fig. 5: Example of application of LSB multi-secret steganography with values histograms. (a) Original image, (b) container including false secret, (c). container including real secret, (d). container including false and real secrets

As noted, the permutation is dependent on the secret key. Therefore, receiver and sender are required to employ the identical sequence. As shown in first example, the key use might be on the basis of the false message digest. The purpose was hiding image given in Figure 4a, but its size is larger than the capacity of the carrier. Hence, some strategic objects were selected from the picture (Fig. 6a). Then, it was saved as Scalable Vector Graphics (SVG) file (Fig. 6b) and encrypted. It was helpful for the reduction of the real message size to almost 1/3 of the original size. The false message is injected into the header, so ASCII text file (2407 characters) is utilized.

It worth noting that the image quality can be manipulated in JPEG files by formulating a quantization factor. Value of this factor influences both the quality and size of the file. In addition, the file size depends on the size of the false message. Thus, the correct selection of quality factor and length of false message might help to improve undetectability. Figure 7 presents the experimentation results using mentioned approach (size of real message = 4.6 KB; size of false message = 3.4 KB).

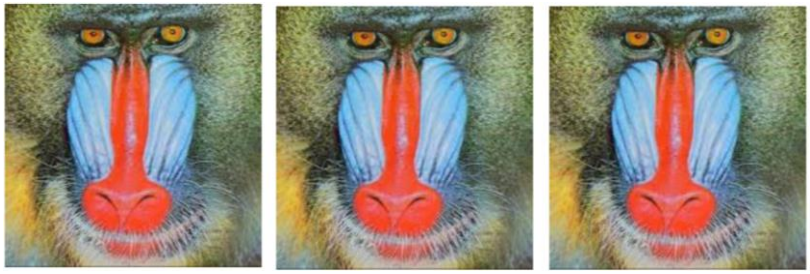
In this situation, embedment of the false secret does not have any impact on the pixel values; it has just an impact on the size of the file. All modifications on the content of the image are presented by hiding the real message. Because of this, containers having one message are not given in separated figure since they are identical to the pure carrier or one with both secrets visually. It is possible also to use F5 algorithm for concealing two various secrets in the coefficients with interlacing. In the proposed method, both types of messages (shorter and longer) are combined prior to shuffling coefficients. It is indicated below. It should be noted that a secret key is necessary – it should be shared by the receiver and the sender. For security, the key used in the coding process should be unlike from the key used in F5.

Algorithm 1

Input: *longMessage*, *shortMessage*, *Key* (array of bytes)
Output: *data* (array of bytes)
1: Compute *lengthL* and *lengthS* (length of *longMessage* and *shortMessage*
2: Use *key* to find permutation *P* from 0 to *lengthL*-1
3: *P*1= *lengths* first element of *P*
4: *P*2= sorted *P*1
5: Create empty data array of length *lengthL* + *lengthS*
6: **for** every *i* = 0…… *lengthS*-1 **do**
7: *index* = *P*2[*i*]+*i*
8: *data*[*index*] = *shortMessage*[*i*]
9: Fill not used places in data array with bytes of *longMessage*
10: **return** data

(a) (b)

Fig. 6: Decrease of secret information size. (a). Selection of interesting regions of image. (b). Real secret (vector image)



(a) (b) (c)

Fig. 7: Example of JPEG multi-secret steganography application. (a) cover image (48.4 KB), (b) stego image (37.0 KB), quality = 89 and (c) stego image (76.1 KB), quality = 100

In the same way as F5 method, the output data are embedded. Permutation in F5 spreads information through the image, so the order of byte is not kept. For this reason, basic shifting is acceptable. In this execution, Length (L) is located on the array start as it is required for decoding secrets. Algorithm 2 shows the way of improving messages from data taken from coefficients.

Algorithm 2

Input: *data*, *Key* (array of bytes), *lengthL*
Output: *longMessage*, *shortMessage* (array of bytes)
1: *lengthS* = length of data - *lengthL*
2: Create empty arrays
3: *longMessage* of length *lengthL*
4: *shortMessage* of *lengthS*
5: Use key to find permutation *P* from 0 to *lengthL*-1
6: *P*1 = *lengthS* first elements of *P*
7: *P*2 = sorted *P*1
8: **for** every *i* = 0,….. *lengthS*-1 **do**
9: index = *P*2[i]+*i*
10: *shortMessage*[*i*] = *data*[*index*]
11: Fill *longMessage* array with unused bytes from data array
10: **return** *longMessage*, *shortMessage*

Two secrets were hidden in a single container, which were encrypted images that was already indicated in Fig. 4b (longer message) and Fig. 6b (shorter message). The "1421974" and "Science" were used as the key for coding/decoding and F5 permutation algorithms, respectively. Figure 8 indicates the experimental results. The selected quality factor influences size of file and, thus, it affects available capacity. The results of experiments are presented in Figure 9. The chosen quality factor affects file size and, therefore, available capacity.

The other method is using more than one level steganography and inserting the secret information on the higher level. Steps of this method are as follows. Firstly, encrypted SVG file from Fig. 6b is hidden in the digital image shown in Fig. 5a. In the next step, the again created object (Fig. 10b) is employed as the next secret and it is inserted in another container (Fig. 10a). Figure 10c indicates the final result. Figure 10d presents the impact of dropping the first step and using just images from Fig. 5a and 10a. It should be mentioned that the capacity is limited by every level of multi-level steganography. In this example, the size of the secret information is 4.6 KB and the movers' sizes are 46.4 and 422.5 KB on level 1 and level 0. Below there are characteristics of the most important features of described techniques of multi-secret steganography.

False LSB Steganography

In this approach, the false message is hidden constantly in LSB of all components. Real message is embedded in second LSB of blue and red component with permutation specifically. Thus, the present capacity is 1/8 of size of carrier for the false secret and the capacity is 1/24 for the real one (assuming 24-bit pixel).

False JPEG Steganography

Using F5 algorithm, real secret is embedded. This algorithm has a capacity of about 14.4% of the size of the carrier (Belazi *et al*., 2016). There is a complicated attack allowing the message length estimation. Steganalysis approaches are simple, for instance, verifying file header or replacing comment for the destruction of the message.

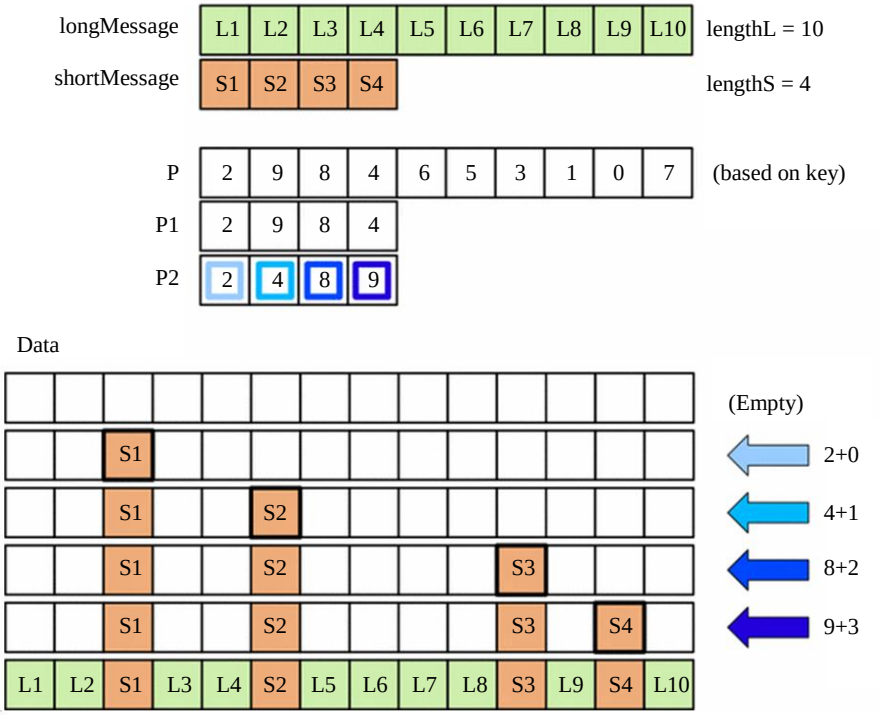


Fig. 8: Example of algorithm 1

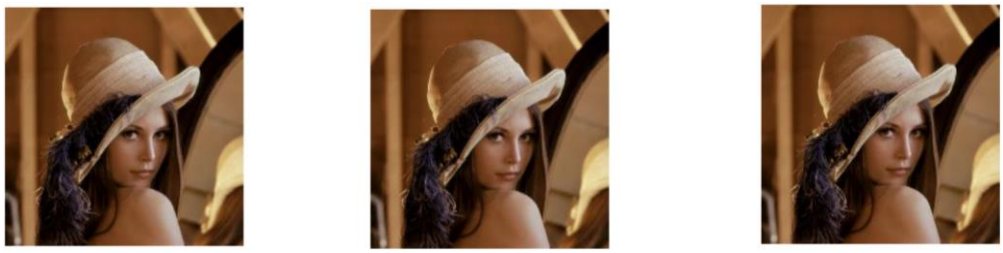


Fig. 9: Example of F5 multi-secret steganography application. (a) Original image (412.5 KB), (b) stego image (271.3 KB), quality = 88 and (c) stego image (735.5 KB), quality = 100

Fig. 10: Example of F5 multi-level steganography application. (a) Level 0 container, (b) level 1 container with secret message, (c) level 0 container with embedded (b) and d level 0 container with embedded

Table 1: Carrier capacity for real and false secret

Method name	False message	Real message
False LSB steganography	14.5% (1/8)	6.17% (1/24)
False JPEG steganography	15.4% (Fridrich *et al*., 2003)	Unlimited
Multi-level F5 steganography	(0.13)n+1×100% on level n (for both real and false messages)	

Multi-level F5 Steganography

For hiding the current secret, F5 algorithm is employed on every level. The present capacity is required to be calculated independently for every level. As just one approach was utilized, the capacity estimated on level n is (0.13) n+1×100% of the size of the container. Potential attacks are the same as those defined for false JPEG steganography with the difference that the second part, as in this case, the header, stays intact. Table 1 summarizes the available capacity of the presented approaches.

Conclusion and Future Work

The multi-level secret steganography concept described in the current work can be applied in many situations. In the cases that communication place between the sender and the receiver is monitored, any container change is disposed so embedding the false message can be a select. When the possibility of examination the transmitted data by warden is very low, there is no need for using false steganography. The main aspects that should be taken into account in design of an appropriate steganographic algorithm include maximum embedding capacity, imperceptibility and satisfactory security level (eaves dropper's inability for detection of hidden data). It is anticipated that the new approaches meet these requirements and provide lower computational complexity. The most suitable approaches for specific situations should be indicated. When supervisor suspects about usage of steganography, it is possible that the carrier will be tested for potential availability of hidden data. False steganography is the best selection in this case. This select can be correct as follows. The false message embedding introduces the largest alterations of the container. Hence, statistical anomalies happen during steganalysis in that place. It implies that basic data are hidden there. Multi-level steganography can be considered when the secret is relatively small. When there is more than one important message, mixing the secrets and hiding them with hard is a reasonable solution to detect approach. Then, messages can also be treated as real secret and the above approach can be applied along with another method proposed in the current paper.

The growth of modern communication needs a special means of security especially on computer network. As there appears a risk that the sensitive information transmitted might be intercepted or distorted by unintended observers for the openness of the internet. So it has resulted in an explosive growth in secure communication and information hiding. Moreover, the information hiding technique can be used extensively in applications like business, military, commercials, anti-criminal, digital forensic and so on.

Acknowledgement

I am heartily thankful to my supervisor Prof. Dr. Muzhir Shaban Al-Ani, whose encouragement, guidance and support from the initial to the final level of this study enabled me to develop an understanding of the subject. Gratitude is also extended to my friends for their help and contributions. I am also indebted to my parents for their unfailing confidence and support in everything I do. I would like to thank my family for their support.

Ethics

A significant contribution to the work reported. This could be in terms of research conception or design, or acquisition of data, or the analysis and interpretation of data.

References

Ansari, S., N. Gupta and S. Agrawal, 2012. An image encryption approach using chaotic map in frequency domain. Int. J. Emer. Technol. Adv. Eng., 2: 287-291.

Bailey, K. and K. Curran, 2005. Steganography. The art of hiding information. Book surge Publishing.

Belazi, A., A.A. Abd, E. Latif and S. Belghith, 2016. A novel image encryption scheme based on substitution-permutation network and chaos. Eur. Assoc. Signal Proc., 128: 155-170. DOI: 10.1016/j.sigpro.2016.03.021

Budhia, U., D. Kundur and T. Zourntos, 2006. Digital video steganalysis exploiting statistical visibility in the temporal domain. IEEE Tran. Inform. Forensics Security, 1: 502-516. DOI: 10.1109/TIFS.2006.885020

Castiglione, A., A. De Santis and C. Soriente, 2007. Taking advantages of a disadvantage: Digital forensics and steganography using document metadata. J. Syst. Softw., 80: 750-764. DOI: 10.1016/j.jss.2006.07.006

Castiglione, A., A. De Santis, U. Fiore and F. Palmie, 2012. An asynchronous covert channel using spam. Comput. Math. Applic., 63: 437-447. DOI: 10.1016/j.camwa.2011.07.068

Castiglione, A., B.D. Alessio and A. De Santis, 2011a. Steganography and secure communication on online social networks and online photo sharing. Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Oct. 26-28, IEEE Xplore Press, Barcelona, Spain, pp: 363-368. DOI: 10.1109/BWCCA.2011.60

Castiglione, A., D. Alessio B. De Santis and A.F. Palmieri, 2011b. New steganographic techniques for the OOXML file format. Proceedings of the IFIP WG 8.4/8.9 International Cross Domain Conference on Availability, Reliability and Security for Business, Enterprise and Health Information Systems. (HIS '11), Springer, Berlin, Heidelberg, pp: 344-358. DOI: 10.5555/2033973.2034003

Castiglione, A., A. De Santis, U. Fiore and F. Palmieri, 2011c. E-mail-based covert channels for asynchronous message steganography. Proceedings of the 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Jun. 30-Jul. 2, IEEE Xplore Press, Seoul, South Korea, pp: 503-508. DOI: 10.1109/IMIS.2011.133

Dianconu, A.V., 2016. Circular inter-intra bit-level permutation and chaos-based image encryption. Inform. Sci., 355: 314-327. DOI: 10.1016/j.ins.2015.10.027

Fridrich, J.J., M. Goljan and D. Hogea, 2003. Steganalysis of JPEG images: Breaking the F5 algorithm. Proceedings of the 5th International Workshop on Information Hiding, Oct. 7-9, Springer, London, pp: 310-323. DOI: 10.1007/3-540-36415-3_20

Lahrod, H.H., A. Rahnemaei and H. SeyyedHatami, 2016. A new method for encrypting digital data using symmetric key in information exchange spaces. Int. J. Comput. Applic. Technol. Res., 5: 391-394. DOI: 10.7753/IJCATR0506.1012

Li, X., C. Li and I.K. Lee, 2016. Chaotic image encryption using pseudo-random masks and pixel mapping. Eur. Assoc. Signal Proc., 125: 48-63. DOI: 10.1016/j.sigpro.2015.11.017

Liu, W., K. Sun and C. Zhu, 2016. A fast image encryption algorithm based on chaotic map. Opt. Lasers Eng., 84: 26-36. DOI: 10.1016/j.optlaseng.2016.03.019

Norouzi, B. and S. Mirzakuchaki, 2016. Breaking an image encryption algorithm based on the new substitution stage with chaotic functions. Optik Int. J. Light Electron Opt., 127: 5695-5701. DOI: 10.1016/j.ijleo.2016.03.076

Tang, Z., J. Song, X. Zhang and R. Sun, 2016. Multiple-image encryption with bit-plane decomposition and chaotic maps. Opt. Lasers Eng., 80: 1-11. DOI: 10.1016/j.optlaseng.2015.12.004

Zhi-Liang, Z.H.U., W.A.N.G. Chong, C.H.A.I. Hua and Y.U. Hai, 2011. A chaotic image encryption scheme based on magic cube transformation. Proceedings of the 4th International Workshop on Chaos-Fractals Theories and Applications, Oct. 19-22, IEEE Xplore Press, Hangzhou, China. DOI: 10.1109/IWCFTA.2011.75