Acta Polytechnica **59**(2):126–133, 2019
doi:10.14311/AP.2019.59.0126

available online at http://ojs.cvut.cz/ojs/index.php/ap

A NEW AND ADAPTIVE SECURITY MODEL FOR PUBLIC COMMUNICATION BASED ON CORRELATION OF DATA FRAMES

Haider Tarish Haider[a,*], Dhiaa Halboot Muhsen[a], Haider Ismael Shahadi[b], Ong Hang See[c]

[a] *University of Mustansiriyah, Department of Computer Engineering, 10001 Baghdad, Iraq*

[b] *University of Kerbala, Department of Electrical and Electronic Engineering, 56001 Karbala, Iraq*

[c] *Universiti Tenaga Nasional, Department of Electronics and Communication Engineering, 43000, Selangor, Malaysia*

[*] corresponding author: haiderth@uomustansiriyah.edu.iq

Abstract. Recent developments in communication and information technologies, plus the emerging of the Internet of Things (IoT) and machine to machine (M2M) principles, create the need to protect data from multiple types of attacks. In this paper, a secure and high capacity data communication model is proposed to protect the transmitted data based on identical frames between a secret and cover data. In this model, the cover data does not convey any embedded data (as in normal steganography system) or modify the secret message (as in traditional cryptography techniques). Alternatively, the proposed model sends the positions of the cover frames that are identical with the secret frames to the receiver side in order to recover the secret message. One of the significant advantages of the proposed model is the size of the secret key message which is considerably larger than the cover size, it may be even hundred times larger. Accordingly, the experimental results demonstrate a superior performance in terms of the capacity rate as compared to the traditional steganography techniques. Moreover, it has an advantage in terms of the required bandwidth to send the data or the required memory for saving when compared to the steganography methods, which need a bandwidth or memory up to 3-5 times of the original secret message. Where the length of the secret key (positions of the identical frames) that should be sent to the receiver increases by only 25% from the original secret message. This model is suitable for applications with a high level of security, high capacity rate and less bandwidth of communication or low storage devices.

Keywords: Covert communication, information hiding, high capacity, high transparency, steganography, encryption.

1. Introduction

The growth in the communication networking has led to a high data transfer rate among public networks [1–3]. Recently, more and more applications for the data communication contribute to the everyday life and become an inseparable part of it [4], such as medical health networks [5], Internet of Things (IoT) [6], vehicle networks communication, smart grid [7], cloud computing, etc. [8, 9]. Most of these applications perform over public networks, while some of these data are effective or very important in terms of the user point of view [10]. Therefore, security techniques are very important to protect data from unauthorized users [11]. The standard solutions for the data security are cryptography and steganography. The cryptography deals with techniques that change the original secret message into another form of data to make it incomprehensible to unauthorized users [12, 13]. The steganography hides the data of a secret message into cover media to prevent drawing any suspicion to the secret data [14, 15]. In the literature, there are many researches in the cryptography field. In [16], a book ciphering is introduced with different examples. However, the security of book ciphering is still poor because the entropy per character of both the plaintext and the running key is low and the combining operation is relatively easily inverted. In [17], the authors proposed a processing system for privacy-preserving data by employing homomorphic in seven of basic operations over the cipher texts scheme. In [18], an information encryption method based on the diffractive imaging by introducing the customized data container was proposed. In this method, the primary information was transformed into the customized data container before being encrypted with the diffractive-imaging-based encryption. A reversible data hiding scheme through the image encryption and support vector machine based data extraction and image recovery scheme was proposed in [19]. This scheme provides a way for a secure medical image transmission. The electronic patient record, which contains basic details about patients, can be embedded into the medical images itself, instead of sending it as a separate file. In [20], an image encryption based on a diffraction

imaging of mixed state was presented. Consequently, colour image layers, R, G, and B, were encrypted and combined together in a single grayscale image using a classical encryption of an optical phase mask. In [21], the authors introduce an optical encryption system based on a single-shot-ptychography encoding (SPE) technique and quick response (QR). The QR codes are encrypted into cipher text through the SPE and visual cryptography. In [22], an automatic encryption scheme based on the neural networks is investigated according to the basic symmetric key model. The results showed that the security solutions based on the advanced deep learning techniques may start to play an important role in the future related directions.

In contrast, there are also many steganography approaches, which recently have been proposed, to hide secret messages in order to prevent the access of unauthorized receivers to the secret messages. In [14], a lossless adaptive embedding for JPEG images was proposed. The proposed method in [14] investigated the relations of the used and the unused variable-length-code (VLCs), consequently. The code mapping and reordering are used to construct the data embedding, the embedding rate was increased by a constructing mapping between the used and unused Huffan codes. An adaptive covert communication model was presented in [23]. The model employed the possibility of an available similarity among the discrete speech samples to reorder the wavelet coefficients of a secret speech and any other speech. Subsequently, the adaptation vector that contains the original index location of the secret speech samples was sent to the receiver as an alternative of the encrypted message or a cover signal. However, both the quality of the reconstructed data and capacity rate were low. Both Finite Ridgelet Transform (FRT) and Discrete Wavelet Transform (DWT) were employed in [24] as a hybrid domain for the image steganography. The FRT was applied for a cover image to get ridgelet coefficients of each layer of the cover, then, a single level DWT was applied to get four bands for each layer. This has been further modified by encrypting the layer value of a secret colour image to get a stego colour image. A coverless information hiding method based on compound words was proposed in [25]. The compounds synthesized method was used by two neighboring keywords as the secret information. After that, the binary numbers are used as the location tags to retrieve the carrier texts in the testing database. It is worth to mention that the carrier texts include the location tags and the compounded keywords In [26], an adaptive least significant bit (LSB) substitution method using an uncorrelated colour space was used in order to increase the property of imperceptibility while minimizing the noticeability by the human vision system. The secret messages were encrypted using an iterative magic matrix encryption algorithm (IMMEA) to increase the level of security, producing the cipher contents.

It is observed that most of the above presented works for both cryptography and steganography have their limitations. In encryption, the encrypted messages create suspicions information and attract the attention of attackers. In contrast, information hiding (steganography) require a trade-off among the level of security, embedding rate and quality. Therefore, this study tries to overcome most of the drawbacks for both encryption and steganography. The proposed model in this study presents a new model to provide a high capacity and secure data communication model. This is realized by sending the data without embedding any secret message into a cover image to prevent any type of suspicious. Accordingly, this increases the capacity rate and keeps a high quality of the cover images.

The rest of the paper is organized as follows. In section 2, the proposed model is described in detail. The results and discussion of the proposed model are presented in section 3. Finally, the conclusion is given in section 4.

2. The proposed model of secret communication

The proposed secure communication model does neither hides the secret message in a cover nor encrypts the secret message. The proposed model is based on scanning identically between cover and secret frames. Subsequently, the positions of the identical cover frames, which are completely similar to the secret message frames, are send to the receiver side. Accordingly, the authorized receiver can easily detect the secret message based on the cover image, which is saved in his database. The following subsections illustrate the proposed model in details:

2.1. Transmission phase of the proposed model

The transmission phase of the proposed security model is designed to be simple and compatible for any type of secret message, such as images, texts, speech, etc. It involves three main stages, the secret message pre-processing, cover image pre-processing and localizer of identical data. Fig. 1 illustrates the main three stages of the transmission phase.

In order to illustrate the overall model in the transmitter side, we assume the secret message is a grayscale or one array of RGB image $S\,(i,j)$ pixels, where $i = 1,\ldots,N$, and $j = 1,\ldots,M$. This image is converted into a binary vector form $S_{BV} = S(f)$ bits, $f = 1\ldots N \times M \times 8$.

Regarding the cover image $C(L,H)$ with $L \times H$ pixels, the same process has been applied to get the final vector form of the cover image data. These data are arranged as a vector form instead of matrix form to minimize the key length. $C_{BV} = C(q), q = 1,\ldots,L \times H \times 8$.

Afterwards, both the cover and the secret data vectors are available for the next step that checks the

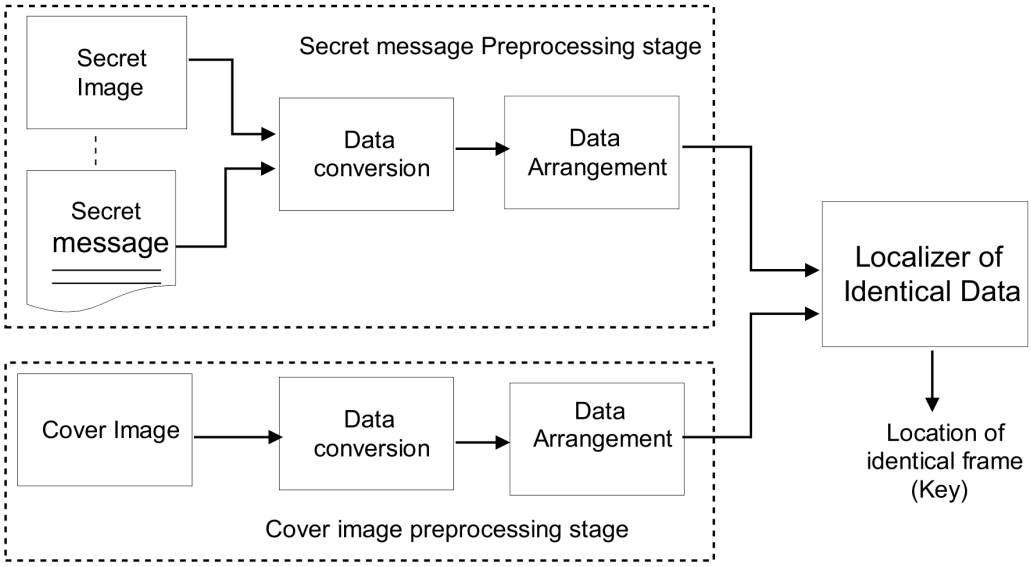

Figure 1. Transmitter phase of the proposed security model.

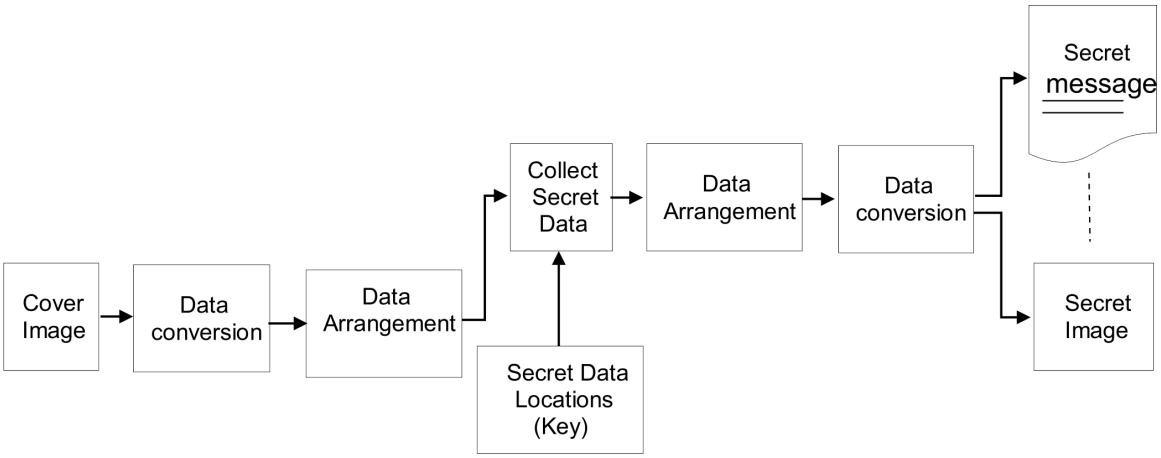

Figure 2. The extraction process of proposed model.

availability of the identical data of the cover image with the secret message frames. The model adapts the selected length of the secret message frame (SMF) to be identical with the cover image data based on the minimum ratio of key (K) to the secret message length.

$$SMF = [1, 2, \ldots, n] \tag{1}$$

subject to minimum (K/SML) where K is the length of the key, and SML refers to the Secret Message Length.

For each selected secret frame length, the proposed model evaluates the similarity condition of completely similar frames (100% available) between the cover and secret data. The final location vector of the optimal length of the selected secret frame is stored as a key for the extraction process. This key satisfies the condition for the minimum length of the key to the secret message length.

Moreover, the data key should be sent to the received side by any type of communication media.

$$K = \left[L_1, L_2, \ldots, L_{((N\times M)/SML)}\right] \tag{2}$$

where L_1 is the location of the first secret message frame into the cover image and so on.

2.2. Secret message extraction (receiver phase) of the proposed security model

In the reception phase, the location vector of the similar data between the secret and cover frames should be available in order to recover the secret message as shown in Fig. 2. In the first stage, the cover image is converted into binary data and then rearranged into a vector form to produce C_{BV} as in the transmission process. In the second stage, by using the location vector key K as in (2), the reconstructed secret messages are collected from the cover data vector RS_{BV}, where RS_{BV} is the reconstructed binary form of the secret message. Third stage starts by rearranging the vector form of the collected secret message into a matrix form. RS_{BM}. Finally, the secret message is

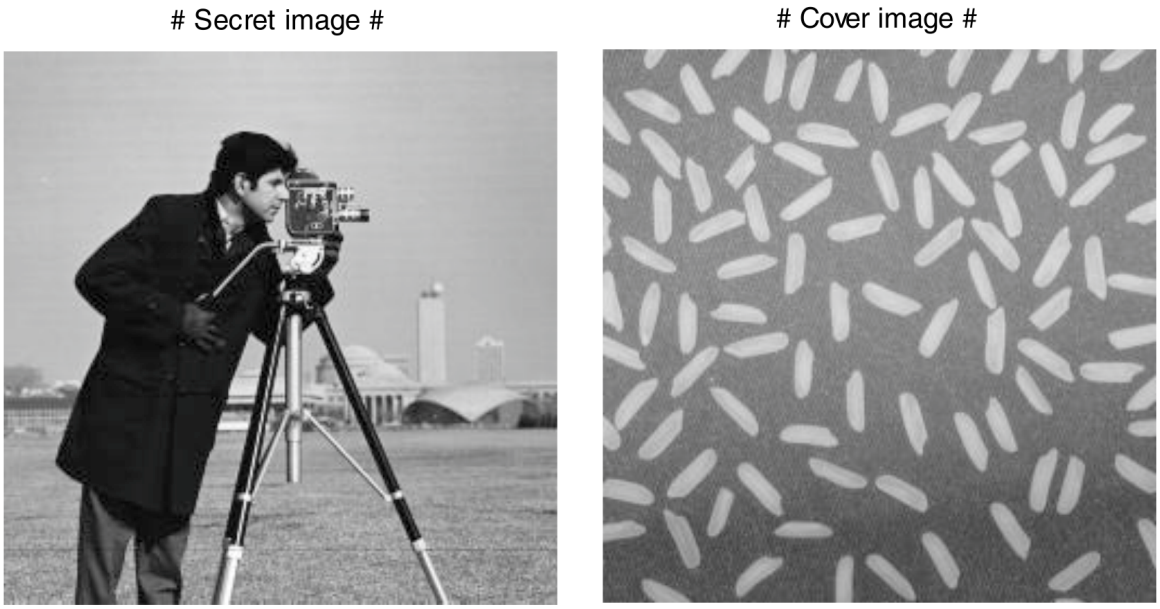

FIGURE 3. (a) Secrete image, (b) Cover image.

converted into the original form of data (text, image, etc).

3. Results and discussion

The proposed model is tested for two types of secret messages (images, text) with a different size of cover images using MATLAB software packages. The secret message frame length (SMF) in (1) is adaptive based on the condition presented in (1) provided that 100% similarity between the secret message frames and cover image data is kept. To emphasize the superiority of the proposed model in terms of the high capacity feature, different percentage values of the secret to cover message length have been tested. The normalized correlation (NC) is used to test the similarity between the original and the reconstructed secret message as in (3) [24]. The performance of any security techniques is perfect if NC value is 1.

$$NC(org, rec) = \\ = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} org_{i,j} rec_{i,j}}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{M} org_{i,j}}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{M} rec_{i,j}}} \quad (3)$$

Different types of images are selected from the MATLAB database to test the proposed model. First, the cameraman (256×256) is selected as a secret image and the rice (256×256) as a cover image as shown in Fig. 3 (a) and (b) respectively. The results of the given cover and secret images are presented in Table1. Based on table 1, the rate of the size of the secret message (image) to the cover image is taken from a similar size 1:1 up to 1:600 times (which means the secret image is bigger than the cover image by 600 times) to highlight the capacity of the proposed model.

FIGURE 4. The reconstructed secret image cameraman (256×256).

As listed in this table, for a similar size, 1:1, the optimal length of the secret message frame is 3 bits with a percentage of the secret message to key length of 1.33. For a high capacity of 1:600 times, the optimal SMF is 7 for the same ratio of the key to secret message length of 1.3. It is worth to mention that, for all data, the similarity of the secret message is completely available in the cover image data. Furthermore, the NC for the reconstructed secret image is 1, which means there is no data loss in the proposed model. Fig. 4 shows the reconstructed secret image.

Table 2 shows the results for the colour secret image of Autumn (345×206) and the cover image Office_4 (903×600) as shown in Fig. 5. Based on one array of

Optimal SML (bits)	Secrete image / Cover image size (%)	K/Secret message length	NC
3	1	1.33	1
3	10	1.33	1
8	50	1.33	1
3	100	1.33	1
6	300	1.33	1
7	600	1.33	1

Table 1. Results of cameraman secret image and the rice cover image.

Optimal SML (bits)	Secrete image / Cover image size (%)	K/Secret message length	NC
6	1	1.33	1
4	10	1.25	1
8	50	1.37	1
7	100	1.42	1
6	300	1.5	1
6	600	1.5	1

Table 2. Results of Autumn cover image and the Office_4 secret image.

Optimal SML (bits)	Secrete text size / Cover image size (%)	K/Secret text length	NC
3	Original size for each	1.33	1
3	10	1.33	1
6	20	1.49	1
3	30	1.33	1
4	40	1.25	1

Table 3. Results of Rice cover image and the text secret message.

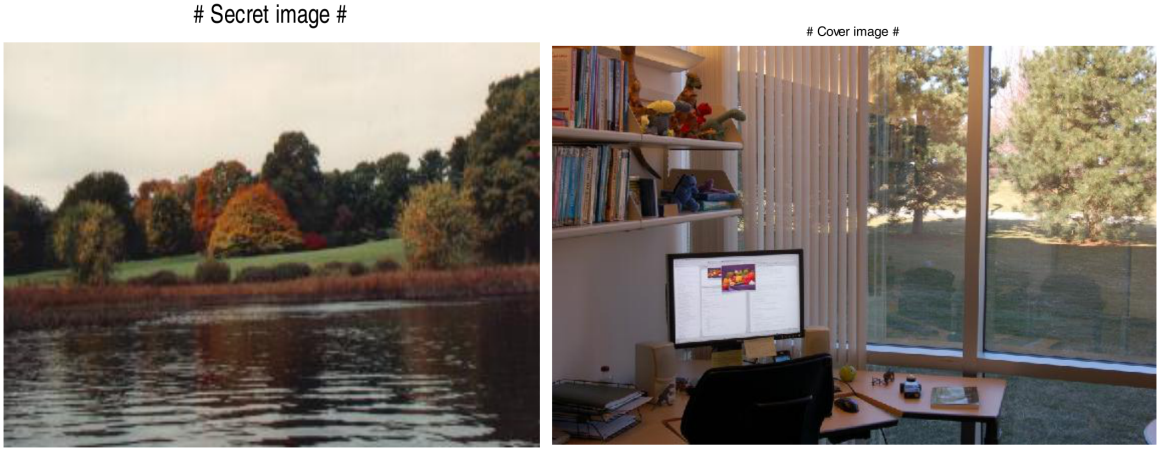

Figure 5. (a) Secrete image, (b) Cover image.

FIGURE 6. The reconstructed secret image autumn (345 × 206).

Cover image	Secret image	NC
Cameraman	Rice	0.003
Autumn	Office	0.006
Rice	Text	0.001

TABLE 4. Results of key change sensitivity.

cover and secret images, the minimum secret message to key length is presented in 10% of the rate of the secret message to cover image size for an optimal secret message frame of 4 bits. For the very high capacity of 1:600 ratio of the secret image to the cover image size, the secret message to key length is about 1.5. Furthermore, the NC for all sizes of images are equal to 1. Fig. 6 shows the reconstructed image.

The proposed model is tested for a text type that contains 1055 different patterns and each pattern has 8 bits (1 byte) as a secret message while the cover image is is represented by a rice photo of (256 × 256) pixels. Table 3 shows the results for different percentages of text to cover image size.

For a high capacity of 40% secret to cover image size, it gives a very low ratio of key to secret message length of about 1.25.

3.1. Performance evaluation of proposed model

Based on the proposed model, the cover image is sent without any modification so that imperceptibility performance (quality of image) is not affected.

Analysing the security of the proposed model against different types of attacks is achieved through different stages. First step is to test the key immunity of the proposed model against key change. Based on robustness of the secure system, a high sensitivity should be presented to the change into the secret key [27]. In this scenario, let us suppose the cover image is available but the secret key not detected, the reconstructed secret messages from the adapted key for different types of cover and secret images draw a high sensitivity for the key change as shown in Table 4.

Cover image	Secret image	NC
Office	Rice	0.009
Rice	Office	0.008
Cameraman	Text	0.006

TABLE 5. Results of cover change sensitivity.

From these results, the proposed model is secure and has a high sensitivity for the key change.

The second test for the sensitivity of the proposed model is focused on the cover image changes. For this case, let us suppose that the key is available but the cover image is not recognized. Different cover images from the original one that has been used in the sending process, have been used for reconstructing the secret message. Table 5 shows the results of this scenario, the results show a high sensitivity for the cover image change to reconstruct the secret message.

3.2. High level of security and capacity rate of process model

In steganography, the level of security (undetectability) depends on how many secret message size hide into cover message (embedding capacity) and imperceptibility (visual quality). These evaluation parameters counteract one another. While, in cryptography that focus on modification of a secret message to make it incomprehensible to illegal users. In cryptography, the level of security depends on the exhibit high sensitivity to a secret key.

The proposed security model does not deal with steganography techniques because there are no information hiding in the cover message nor cryptography techniques. The cover message is sent without any change in its original form so as there be no arising for any type of suspicious, change or modifying to the cover data. This lead to very high level of security for the information transmission over a common communication media. Furthermore, the capacity rate for secret information are very high as compared to cover information. Therefore, the proposed model overcomes the overhead of maintaining high level of security and high capacity rate that can be obtained via the available security techniques in steganography and cryptography.

3.3. Comparison of proposed model with existing models

The available data security techniques in literature are classified into two categories; encryption and information hiding. The proposed method differs from these two techniques.

Therefore, a basic comparison with these works is maintained here. Several significant features are highlighted. The most important feature is the capacity rate (CR), which refers to the possible frames of the secret message that can be exactly located in the cover image.The capacity rate in the proposed model

Methods	CR	NC
[24]	1	1
[23]	1	0.95
proposed	600	1

Table 6. Results of comparison.

slightly differs from the information hiding approach, where, in information hiding, the capacity rate refers to the amount of embedding data capacity into the cover. In steganography, a high capacity rate requires 3-4 times of the secret message size [23]. Furthermore, steganography methods of high capacity have a very weak robustness and critical imperceptivity. While in the proposed model, there is no information hiding into the cover image. Table 6 shows the comparison of the capacity rate of the proposed model with other works regardless the types of secret and cover messages. From table 6, it can be seen that the proposed model provides very high capacity rate. Most algorithms in the literature have a capacity rate lesser than 1 time the secret image since the quality of images are affected.

4. Conclusion

In this paper, a secure data communication model based on adaptive identical data frames is proposed for a high capacity rate and image quality. In this model, the cover image is sent to the receiver without any modification to prevent any suspicion from attackers and to keep a high imperceptibility. Based on the optimal length of the secret message, the last can be identically identified in the cover image. Accordingly, the location of these data is sent to the receiver side in order to reconstruct the original secret message. The capacity of the secret message can be larger than the cover image, up to 600 times. While the length of the key is not larger than the secret message by more than 25%. The results of the proposed model are evaluated and compared with other works in terms of the capacity rate and quality of the reconstructed secret message. It is found from the comparison that the proposed model achieves superior findings and combines the advantages of steganography and cryptography techniques of high capacity rate and high quality.

Acknowledgements

The first and second authors would like to thank Mustansiriyah University (`www.uomustansiriyah.edu.iq`) Baghdad-Iraq for its support in the present work.

References

[1] M. Hussain, A. Wahid, N. Javed, K.-H. Jung. Recursive Information Hiding Scheme Through LSB, PVD Shift, and MPE. *IETE Technical Review* **35**(1):53–63, 2018. doi:10.1080/02564602.2016.1244496.

[2] S. A. El Rahman. A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information. *Computers & Electrical Engineering* **70**:380 – 399, 2018. doi:10.1016/j.compeleceng.2016.09.001.

[3] S. Jia, Q. Zhou, H. Zhou. A novel color image watermarking scheme based on DWT and QR decomposition. *Journal of Applied Science and Engineering* **20**:193–200, 2017. doi:10.6180/jase.2017.20.2.07.

[4] I. Muslukhov, S.-T. Sun, P. Wijesekera, et al. Decoupling data-at-rest encryption and smartphone locking with wearable devices. *Pervasive and Mobile Computing* **32**:26–34, 2016. doi:10.1016/j.pmcj.2016.06.016.

[5] X. Liao, J. Yin, S. Guo, et al. Medical JPEG image steganography based on preserving inter-block dependencies. *Computers & Electrical Engineering* **67**:320–329, 2018. doi:10.1016/j.compeleceng.2017.08.020.

[6] L. Atzori, A. Iera, G. Morabito. The Internet of Things: A survey. *Compututer Networks* **54**(15):2787–2805, 2010. doi:10.1016/j.comnet.2010.05.010.

[7] S. Reddy, M. Kumar, T. Mallick, et al. A review of integration, control, communication and metering (ICCM) of renewable energy based smart grid. *Renewable and Sustainable Energy Reviews* **38**:180–192, 2014. doi:10.1016/j.rser.2014.05.049.

[8] D. Zeng, S. Guo, Z. Cheng. The web of things: A survey (invited paper). *Journal of Communications* **6**(6):424–438, 2011. doi:10.4304/jcm.6.6.424-438.

[9] L. Xue, Y. Yu, Y. Li, et al. Efficient attribute-based encryption with attribute revocation for assured data deletion. *Information Sciences* **479**:640–650, 2019. doi:10.1016/j.ins.2018.02.015.

[10] G. Hamed, M. Marey, A. S. El-Sayed, M. Tolba. Hybrid, randomized and high capacity conservative mutations DNA-based steganography for large sized data. *Biosystems* **167**:47–61, 2018. doi:10.1016/j.biosystems.2018.03.003.

[11] M. Kowalski, M. Życzkowski. Encryption method based on pseudo random spatial light modulation for single-fibre data transmission. *Optics Communications* **402**:401–407, 2017. doi:10.1016/j.optcom.2017.06.046.

[12] L. Zou, J. Sun, M. Gao, et al. A novel coverless information hiding method based on the average pixel value of the sub-images. *Multimedia Tools and Applications* pp. 1–16, 2018. doi:10.1007/s11042-018-6444-0.

[13] T. Aura. *Lecture Notes in Computer Science*, vol. 1174, chap. Practical Invisibility in Digital Communication, p. 265–278. Springer, 1996. doi:10.1007/3-540-61996-8_46.

[14] Y. Qiu, H. He, Z. Qian, et al. Lossless data hiding in JPEG bitstream using alternative embedding. *Journal of Visual Communication and Image Representation* **52**:86–92, 2018. doi:10.1016/j.jvcir.2018.02.005.

[15] M. Tang, W. Song, X. Chen, J. Hu. An image information hiding using adaptation and radix. *Optik - International Journal for Light and Electron Optics* **126**(23):4136–4141, 2015. doi:10.1016/j.ijleo.2015.07.200.

[16] D. Ristanovic, J. Protic. The book cipher algorithm **33**:46–51, 2008.

[17] W. Ding, Z. Yan, R. H. Deng. Encrypted data processing with homomorphic re-encryption. *Information Sciences* **409-410**:35–55, 2017. DOI:10.1016/j.ins.2017.05.004.

[18] Y. Qin, Z. Wang, H. Wang, et al. Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container. *Optics and Lasers in Engineering* **105**:118–124, 2018. DOI:10.1016/j.optlaseng.2018.01.014.

[19] M. v. M., V. Masilamani. Reversible data hiding scheme during encryption using machine learning. *Procedia Computer Science* **133**:348–356, 2018. DOI:10.1016/j.procs.2018.07.043.

[20] X. He, H. Tao, C. Liu, J. Zhu. Single-shot color image encryption based on mixed state diffractive imaging. *Optics and Lasers in Engineering* **107**:112–118, 2018. DOI:10.1016/j.optlaseng.2018.03.018.

[21] Y. Zhu, W. Xu, Y. Shi. High-capacity encryption system based on single-shot-ptychography encoding and QR code. *Optics Communications* **435**:426–432, 2019. DOI:10.1016/j.optcom.2018.11.040.

[22] L. Zhou, J. Chen, Y. Zhang, et al. Security analysis and new models on the intelligent symmetric key encryption. *Computers & Security* **80**:14–24, 2019. DOI:10.1016/j.cose.2018.07.018.

[23] I. H. Shahadi. Covert communication model for speech signals based on an indirect and adaptive encryption technique. *Computers & Electrical Engineering* **68**:425–436, 2018. DOI:10.1016/j.compeleceng.2018.04.018.

[24] R. Thanki, S. Borra. A color image steganography in hybrid FRT–DWT domain. *Journal of Information Security and Applications* **40**:92–102, 2018. DOI:10.1016/j.jisa.2018.03.004.

[25] X. Chen, S. Chen. Text coverless information hiding based on compound and selection of words. *Soft Computing* p. 1–8, 2018. DOI:10.1007/s00500-018-3286-7.

[26] K. Muhammad, M. Sajjad, I. Mehmood, et al. Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems* **86**:951–960, 2016. DOI:10.1016/j.future.2016.11.029.

[27] S. Li, C. Li, K.-T. Lo, G. Chen. Cryptanalyzing of an encryption scheme based on blind source separation. *IEEE Transactions on Circuits and Systems I: Regular Papers* **55**(4):1055–1063, 2008. DOI:10.1109/TCSI.2008.916540.