IMG-forensics: Multimedia-enabled information hiding investigation using convolutional neural network

Abdullah Ayub Khan¹,² | Aftab Ahmed Shaikh¹ | Omar Cheikhrouhou³ | Asif Ali Laghari¹ | Mamoon Rashid⁴ | Muhammad Shafiq⁵ | Habib Hamam⁶

¹ Faculty of Computer Science, Sindh Madressatul Islam University, Karachi, Sindh, Pakistan
² Faculty of Computing Science and Information Technology, Benazir Bhutto Shahed University Lyari, Karachi, Sindh, Pakistan
³ College of CIT, Taif University, Taif, Saudi Arabia
⁴ Department of Computer Engineering, Faculty of Science and Technology, Vishwakarma University, Pune, India
⁵ Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China
⁶ Faculty of Engineering, Université de Moncton, Moncton, NB, Canada

Correspondence
Muhammad Shafiq, Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China.
Email: srsshafiq@gmail.com

Abstract
Information hiding aims to embed a crucial amount of confidential data records into the multimedia, such as text, audio, static and dynamic image, and video. Image-based information hiding has been a significantly important topic for digital forensics. Here, active image deep steganographic approaches have come forward for hiding data. The least significant bit (LSB) steganography approach is proposed to conceal a secret message into the original image. First, the lightweight stream encryption cryptography encrypts secret information in the cover image to protect embedded information from source to destination. Whereas the encrypted embedded cover information into the carrier of stego-image with the help of the LSB and then transmit. In the proposed investigational scheme, a convolutional neural net is used. A model is trained to detect and extract patterns of image hidden features, encrypted stego-image optimization, and classify original and cover images of steganography. Through the experiment result on the forensic image database for mobile steganography of the Center for Statistics and Application in Forensic Evidence, the overall embedded and extracting that the proposed scheme can achieve information hiding as well as revealing with an accuracy rate of 95.1%. The experimental result shows the robustness of the model in terms of efficiency as compared to other state-of-the-art schemes.

1 | INTRODUCTION

The rapid enhancement in the development of modern communication and information technology made data streaming faster and easier [1, 2]. Thus resulting the transmission of the data unreliable, and which can be easily manipulated, copied, altered integrity, destroyed authenticity, allowed access to ungranted, malicious attacks, eavesdrop, and authorization. However, preventing the secrecy of crucial information [3] either to preserve or transmit over the network is a critical challenge. Information hiding is the technique of steganography for maintaining data secrecy.

Encryption is a data transformation [4], the process of scrambling data in such a way that allow only authorized users to access the information. Data are converted from plaintext to ciphertext, generate key cryptography, and only a legitimate user can decrypt information by providing the authentic key. Image-based data encryption [5] is the intrinsic concept of information security, with most important features such as bulk data capacity and high redundancy. Image encryption is completely different from text encryption; therefore, hard to handle through traditional cryptographic algorithms. Several image-based encryption algorithms proposed to hide information, for example, a new chaotic algorithm, parallel encryption, a hash-based, advanced encryption standard, lightweight stream algorithm, and many more. Initially, an original image is converted into a single block of bytes and then blocks to values. A multilevel distributed image-based encryption [6, 7] is one of the hot topics in image encryption-based information hiding research orientation nowadays to ensure the confidentiality and integrity of the images, essential quantum of work to accomplish by using the tent and logistic map.

Steganography plays a vital role in cover secret data within ordinary, and conceal digital content in order to avoid the
detection of non-secret massages and hidden data extracted from the destination [8]. However, digital content includes static and dynamic images, hide data in the form of text and encrypt before incorporated into the transmission of data stream [9]. The digital image contains various bytes of the critical point of records in the form of image pixels. This type of scheme allows some space to hide confidential steganographic data enclosed in the data file. Through this, we have highlighted the simple procedure of steganography application in which digital information is embedded into an image where least bit is manipulated by least significant bit (LSB) in the data file and covers malicious code within the digital image.

In cyber security, steganography is the most popular mechanism of information hiding among cyber criminals [10]. Thus, the malware used this technique to conceal the malicious code inside the image file, while manipulating the LSB of multimedia files. Malware is activated when programmable code is sent to the targeted users, and it downloads and opens the multimedia-based content including text, audio, image, and video [11, 12]; attackers gain control access over the computer system. Investigating such criminal activities is a challenging problem for forensic researchers. Traditionally, forensic tools are used to investigate the content of multimedia that takes more time to collect, pre-process, examine, analyse, and preserve evidence integrity. That is the reason to use the convolutional neural network (CNN), which provides sophisticated image-based hiding information solution. This makes robust the forensic process of capturing a steganographic image, convert encrypted stream cipher to plain decryption, detect the hidden pattern of secret information, extract features, and classify cover image originality.

This study addresses the topic of multimedia forensic investigation, a modern form of digital image-based information hiding, proper use of steganography, especially LSB for data conceals, encryption through cryptography technique, optimize features and classify images, extract hidden features as well as train learning model with the help of convolutional neural net. These complete packages robust the performance of multimedia investigations. It surveys multiple image-based information hiding schemes of multimedia forensic investigation, embeds data into the communication technology, for example, audios, images, and videos. Furthermore, the process layers of digital forensics perform a vital role such as collect image-based steganography, identify as well as examine each aspect, deeply analyse encrypted critical information, and preserve the integrity of evidence. Experimental results of the proposed novel scheme are compared with other works of image-based information hiding and future work challenges and limitations in the multimedia forensics are also discussed. Moreover, we have analyzed the results of the proposed method and discussed a set of open issues of multimedia forensics that are yet to be addressed.

The rest of the paper is organized as follows. The next section discusses image-based data security and multimedia forensics using image steganography, encryption, and deep neural nets related work. Section 3 demonstrates the complete model framework of information hiding and its extensions, such as preliminary knowledge, proposed image-based information hiding scheme, and complete implementation details. Section 4 focuses on the results of the proposed scheme, and Section 5 briefly discusses the analysis of information hiding and revealing results and compares it with other state-of-the-art methods. Finally, we conclude our paper in Section 6.

2 RELATED WORK

The paper propounded by Tao et al. [13] mainly focused on image steganography. They proposed a robust framework of steganographic JPEG compression while transmitted over the covert communication channel. The paper first obtains channel compress original version of the channel, confidential data embedded into the channel of the compressed image using the JPEG steganographic method and generates stego-images after the transmission.

Hu et al. [14] have highlighted a novel approach of the steganography without embed (SWE). This steganographic approach is based on deep convolutional generative adversarial networks. The method maps secret data into noise vector, trains generator neural nets model, and generate carrier for image based on the vector. In this generation process, no modification or similar operations are required, and the model extractor successfully extracted image information by other neurons of the network after training.

Rajput and Chavan [15] explained the angular transformation concept of image colour channel for data security. In this paper, the LSB steganographic technique is used to conceal secret data into the colour image with the help of red, green, and blue (RGB) channels. The embedded message is extracted by performing the same angular transformation on the receiving side of the stego-image.

Muhammad et al. [16] proposed an image steganography framework for the authenticity of visual content. This model also utilized colour model transformation, TLEA encryption, Morton scanning, and substitution. First, the input image embeds secret information by Morton scan directly with LSB and adds encryption for additional security for high authenticity. Undoubtedly, this scheme performs very well, but there is some minor limitation on the existing spatial domain method. Due to image processing attacks such as scaling, cropping, rotation, noise etc., the stego-image cannot fully recover.

Artiemjew and Kislak-Malinowska [17] were concerned about the encryption of hiding image into image. The hidden information was placed in selected bytes, indiscernible masks, and a fixed degree to mask the presence of steganographic key usage. The paper used the LSB matching method, such as to verify resistance, and the chi-square method. The feature of this scheme is robustness, correct decoding, channel switching, bit masking, tuning the degree of indiscernibility, and preserving file size. This paper also discussed the LSB limitations in image steganography.

A comparative study of the grayscale image steganography method using Chaoo’s encryption, CNN, and GAN was discussed by Qi Li et al. [18]. In this paper, secret information
is encrypted by the use of the Chao algorithm before hiding and converting into a cover image of the same size. The converted image transforms into a stego-image with the help of CNN. This proposed image steganography scheme addresses three main objectives of CNN such as hiding, discriminative, and extracting networks. The experimental results compared with PSNR and SSIM solve leakage of hiding information as well as colour distortion with the highest rate of 98.7% and 42.3, respectively.

Mukherjee and Sanyal [19] demonstrate the procedure of the N-puzzle encryption technique imposing the Arnold transformation on the cover image. The outcome of the process is a scrambling image, ensuring the pixel data and normal orientation. The N-puzzle was applied to the scrambled image for the purpose of enhancing the version of encryption. After the N-puzzle, the insertion technique of mid position value (MPV) was used to embed bits from the images that would generate a form of carrier image, reverting the process. This complete scenario is applied to the qualitative benchmark parameters and the results are analysed.

Solak and Altmüller et al. [20] present a data hiding scheme based on two-step steganography that enhances quality, capacity, security, and efficiency of embedded stego-image protection. First, hidden information is encrypted with the keywords and shifted to provide protection. In the next stage, researchers proposed adaptive LSB+3 type I and type II for hiding encrypted information into the cover image. This scheme provides more security in image steganography with a high rate of accuracy.

Mazureczuk and Wendzel highlight critical forensic limitations on the applied side of steganography, encryption, detection, and extraction process of hidden information from multimedia investigators [21]. After critically reviewing the related work of steganography, stream encryption, CNN, and its extensions, we have analysed some gaps in the multimedia forensic investigation methods for image-based information hiding. In the next section, we present a framework which targets the robustness of investigation performance in terms of the quality of transmitted image, enhanced capture capability, the capacity to store secret information, more security, and boosting the overall performance of multimedia investigation.

3 PROPOSED SCHEME

3.1 Preliminary knowledge

3.1.1 LSB steganography

The LSB is the lowest bit series of the binary number either leftmost or rightmost, transforming image pixel bits into data bits for hiding the necessary details. This approach is quite simple to understand, including the implementation aspect, such as easy embedding of data in hiding and stego-images results. In this method, we have initially used LSB transformation to enhance the quality of embedded optimal bits of secret code of the cover image, assigned each bit position, and shifted towards the rightmost side. After embedding, transmit the cover image of size, bytes of the PNG grid pixels passed randomly based on LSB bit generation. The information of header bits of the cover image is sent directly to the stego-image [1, 22]. In this paper, we have highlighted primary knowledge of the LSB steganography for hiding secret information and they are as follows:

- In an 8-bit grayscale image, every pixel can have 1 in 2 to the power of 8.
- Let us consider $b_i$ as the pixel value of $i$th iteration in the cover image.
- The number of secret code bit(s) embedded is denoted by $|\text{bi}|$.
- An approach of LSB helps to embed $|\text{bi}|$ bit(s) into hi to obtain stego-image $b'_i$.
- Moving forward $(b_{i+1})$th, adjust the stego-image $b'_i$ bit to generate pixel values in two categories, where $p$ is the overriding bit and $q$ is the original bit that changed.
- Mathematically represent the generated pixel values: $(b'_{p}, b'_{q}) = \{b'_{p} = b'_i + 2^p, b'_{q} = b'_i - 2^q\}$.
- Tuning the range of LSB from 0 to $n - 1$.
- The sum of the adjusted $(b'_{p}, b'_{q})$ pixels bit $b''_i$ calculates as: $b''_i = \sum_{i=1}^{n-1} b'_i, 2^i$.
- In the end, replace $b''_i$ with the bi.

After the complete process of LSBs steganography, stego-image is encrypted by a lightweight stream encryption (LSE) method for protection, which is discussed in the next section.

3.1.2 Lightweight stream encryption

The LSE is a multimedia-based encryption algorithm, mainly used for encrypting images and videos data files [23]. This algorithm plays a crucial role in maps systematic cipher of individual plaintext in the image file and transforms into the special symbol. A linear feedback shift register (LFSR) produces a new stream pseudorandom bit for hardware as well as software of multimedia encryption. The shift register (SR) of bit words performs a simple task: it inputs bits value equalling the linear Boolean function values of the remaining bits in the SR. Calculate the LFSR: a feedback function performs negation of OR logical operator bits values of the encrypted cells as follows:

$$\langle g_{L} \rangle = (a_1 \ast g_{L-1}) \oplus (a_2 \ast g_{L-2}) \oplus (a_3 \ast g_{L-3}) \oplus \ldots \oplus (a_L \ast g_{1})$$

Where ‘g’ is the shift register, ‘a’ is the cell position, and ‘L – 1, 2, … so on’ is the content shifted to the next cell.

The formula of the LFSR next generation is calculated as follows:

$$\langle g_{L+1} \rangle = (a_1 \ast g_{L}) \oplus (a_2 \ast g_{L-1}) \oplus (a_3 \ast g_{L-2}) \oplus \ldots \oplus (a_L \ast g_{1})$$
Finally, the overall complete generations of LFRS is calculated as follows:

\[
\left( g_{l+k-1} \right) = (a_1 \ast g_{l+k-2}) \oplus (a_2 \ast g_{l+k-3}) \\
\oplus (a_3 \ast g_{l+k-4}) \oplus \ldots \oplus (a_L \ast g_{k-1})
\]

Stream cipher pseudorandom sequence and quantization are calculated as follows:

\[
t(n - 1) = \mu t(n) [1 - t(n)]
\]

Following is the equation of stream encryption of 32 bits of the ciphertext along with key transmission:

\[
C_k = P_k \oplus D_k \text{ (where ‘P’ is the 32 bits plaintext converted, and ‘D’ is the decrypted secret key).}
\]

3.1.3 Convolutional neural network

The deep neural network technique aims to look for the patterns in the image, extract the right hidden features, a very vast ranging from the analysis domain of image recognition [24]. This paper addresses the analysis influence of nearby pixels in the image with the help of the kernel. A tensor on CNN kept track of the spatial information, and learned critical features such as detection of object edges. However, images were amplified to filter out unwanted data. Due to the high-pass filter, pixel intensity changes very quickly from 0 to 255 bits of the pixel. Following are some critical assumptions of CNN for multimedia investigation [25]:

- The size of an 8-bit grayscale image is 512 × 512 with a 3 × 3 kernel.
- Each kernel has an RGB colour channel.
- Continuous value of 0 and 1 convolute with the image to detect patterns and features.
- For the feature map, the input of 512 × 512 (X) image multiplies with the 3 × 3 kernel (f).
- Mathematical representation of convolutional (Cov2D) is:
  \[
  Z = X \ast f.
  \]
- Applying dot product to the scaler value and shift kernel next to the entire image.
- Add padding (P) zero value to the input image (2D matrix) for the purpose of fitting the image kernel.
- For image size reduction, the pooling layer reduces the number of parameters as shown in Figure 1.
- To normalize the pooling layer, decrease image complexity and computational power.
- Detect hidden patterns of the image and extract crucial information from it, non-linear transformation activation function used: \( A = \text{sigmoid}(Z) \).
The output of image-based information hiding is: \( f(x) = \frac{1}{1 + e^{-x}} \).

### 3.2 Framework of the proposed image-based information hiding

Information integrity, protection, and preservation for multimedia forensic investigation is a vital challenge [26, 27]. Figure 2 presents a framework of image-based information hiding for multimedia forensics in an investigational context. This framework is a complete demonstration of the sharing of the cover image between distinct transmission channels remotely for the sake of information protection and evidence preservation. The multimedia investigator collects original images; pre-process image by analysing the critical aspects such as noise, scaling, rotation, and cropping, and form a place to hide investigational information. Through the proposed image-based embedding technique and transmit evidence distributed in the form of the cover image to the judiciary along with information integrity as well as preservation. The investigator in another place accesses the encrypted cover image from the source, thereby recovering the secret code via the convolutional neural network detection and extraction procedures. The proposed image-based information hiding and forensic scheme robust performance, ensuring the evidence integrity, confidentiality, and protection for multimedia investigators; this method actively automates learning in the digital forensic investigational systems.

### 3.3 Proposed image-based information hiding scheme

In this section, we have illustrated the mechanism of embedding a secret code into the original image. During the pre-processing phase, an individual image with 8 bits of 512 × 512 size and \( 2^{N-1} \times 2^{N-1} \) size is first to conceal to an image with 2 bits and \( 2^N \times 2^N \) size. This embedded information in an image is then encrypted using LSE that is controlled by a linear feedback shift register and map individual cipher systematically. The encrypted image is embedded within the cover image, utilizing the LSB steganographic technique for concealing secret data. In this proposed scheme, we make the assumption that the secret information \( 2^{N-1} \times 2^{N-1} \) is concealed to \( 2^N \times 2^N \), then the size of the cover image is \( S = \frac{1}{2^N} (\sum_{k=0}^{2N-1} s \oplus k) \). The procedure of embedding a message within the image and code encrypted of the presented approach is as follows:

#### Step #1: The secret information of 2-bits and the size of \( 2^{N-1} \times 2^{N-1} \) is embedded in every 8-bits of LSB string within the image and size of \( 2^N \times 2^N \).

#### Step #2: This cover information is transformed into the encrypted image by lightweight stream encryption, and shift bits register (XOR) in the form of linear feedback are as follows:

\[
(s_L) = (a_1 * s_{L-1}) \oplus (a_2 * s_{L-2}) \oplus (a_3 * s_{L-3}) \oplus ... \oplus (a_2 * s_0)
\]

#### Step #3: The systematic map of a cipher of each plaintext in the data file produce the stream cipher pseudorandom quantization and sequence generation as follows:

\[
T(n-1) = \mu T(n) [1 - T(n)]
\]

#### Step #4: The next generation of bits shifts register is calculated as:

\[
(s_{L+1}) = (a_1 * s_L) \oplus (a_2 * s_{L-1}) \oplus (a_3 * s_{L-2}) \oplus ... \oplus (a_2 * s_1)
\]

#### Step #5: This technique utilizes to embed encrypted information into the cover image and a secret stream cipher key generated from the process, as demonstrated in the following algorithms.
We present the proposed hidden information extraction mechanism, utilize convolutional layers (Conv2D) on the image with the value of MaxPooling ($f = 16, 32$), and so on (16 x 16), and maximize pooling ($\varphi$) $2^n \times 2^n$ size to detect patterns. The procedure of feature detection of embedded secret encrypted information of stego-image with the size of $2^{N+1} \times 2^{N+1}$ is successfully performed by the use of deep flatten (f), dense (d), fully connected layer (X), and sigmoid (Z) activation function for proper extraction of evidence along with message integrity as well as secure storage preservation:

Non-linear feature extraction is $f(\chi) = \frac{1}{1 + e^{-x}}$.

The algorithm demonstrates the proposed method of extracting processes of hidden information through the distinct phases of stego-cipher encryption as follows:

**Input:** Encrypted cover image (C), stego-image (S), and stream cipher key (K)

**Output:** Information extraction (E)

$$E = \frac{1}{2^e} \sum_{k=0}^{2^e-1} b \oplus k; \text{ where } b \text{ is equal to 00 in the initial stage}$$

for $k$ is equal to 0 to $2^e - 1$;

if $k_0 = 1$ then $C_0 = S_7$

else if $S_0 \oplus S_2 = 1 \text{ then } C_0 = 1$

else if $S_0 \oplus S_3 = 0 \text{ then } C_0 = 0$

if $k_1 = 1$ then $C_1 = S_{5e}$, end if

else if $S_1 \oplus S_2 = 1 \text{ then } C_1 = 1$

else if $S_1 \oplus S_3 = 0 \text{ then } C_1 = 0$, end if

In this result, we have utilized the procedure of convolutional network for detection of hidden encrypted features of the image and extract embedded secret evidence when reached the destination side of the channel. The process of information extraction, 512 x 512 original-cover image received from the LSE encryption, Conv2D convolutional layer of size 3 x 3, where the value of $f = 16$, and $f = 32$, MaxPooling is used to optimize image and help to extract hidden features as well as to recognize conceal patterns. After Conv2D and MaxPooling, we flatten connected neurons and tuning dense parameters to adjust the threshold value (0, 1) of the sigmoid non-linear activation function by adding weight and bias (–1, 1) as shown in Figure 6.

5 | RESULTS AND DISCUSSION

The obtained experimental results are compared with the other state-of-the-art methods [29, 30, 21] of image-based secret information hiding. Zhou et al. utilized two formal approaches, one is information hiding and the other is digital forensics; the feature of this research was successfully applied for the prevention of multimedia copyright, privacy, security, and protection [29]. But the massive growth of data in the cloud environment creates challenges for forensic experts in this research [29, 21]. With the rapid use of multimedia systems, in the proposed scheme we overcome threats involved in cyberenvironment, manipulating critical information such as transaction details, intellectual rights, and encrypted secrecy integrity, by using stream cipher strategy. Another group of information hiding investigational and forensic experts demonstrate a coverless scenario of information hiding, the feature of this is to enhance the lower capacity (80-bits carrier) to embed secret messages using the average pixel value of sub-images and encrypt by hashing algorithm [30]. The objective is to map the Chinese dictionary hash array in multi-level indexing for retrieving stego-image. By tackling these kind of hiding issues, we have presented a framework that provides more protection, 2 bits in every 8 bits block carrier capacity, high-level encryption, efficient detection, and accurate extraction with a high rate.

6 | CONCLUSION

We have designed and implemented a scheme for digital image steganography, to detect the encrypted data and retrieve hidden information based on the purpose of multimedia forensic investigation and data security using LSB, LSE, and CNN. This avoids unnecessary hurdle as seen in previous methodology
FIGURE 3  Process of embedding secret information using least significant bit (LSB)

FIGURE 4  Procedure of applying LSE encryption of image-based embed information
FIGURE 5  In the process of forensic investigation, first detect the hidden secret data and retrieve embedded hidden information by using convolutional neural network for further forensic incident investigation and preserve protected information.

FIGURE 6  Experimental results demonstrate the rate of accuracy and efficiency to detect and extract hidden secret information for the proposed image-based information hiding and forensic framework by using CNN.
of multimedia investigation. The proposed work facilitates investigators to tackle the entire process of multimedia, especially image-based contents, extract hidden features that would conceal while transmitted from source to destination. The LSB technique of steganography is used to cover the secret data and messages within the data file by altering the pixel values of the image. A lightweight stream encryption cryptography algorithm is used to encrypt this image-based content, and only the legitimate user can access as well as decrypt confidential information. In the end, the large database of stego-images can be optimized, detected, and classified, as well as the hidden features of the evidence are recognized and preserved with the help of deep CNN. The proposed method makes the performance of digital investigation from image steganography more robust to extract hidden information within the image data file. Several methods were proposed for image-based data security, but the experimental results show that this method achieves better multimedia investigational application than other state-of-the-art schemes with an accuracy of 95.1%.

ACKNOWLEDGEMENTS

Dr. Omar Cheikhrouhou thanks Taif university for its support under the project Taif University Researchers supporting project number (TURSP-2020/55), Taif university, Taif, Saudi Arabia.

CONFLICT OF INTEREST

Authors did not have any conflict of interest.

ORCID

Mamoon Rasheed® https://orcid.org/0000-0002-8302-4571
Muhammad Shafiq® https://orcid.org/0000-0003-1909-9373

REFERENCES

1. Nasihat, D., Mamdouh, L.: An efficient steganographic technique for hiding data. J. Egypt. Math. Soc. 27(1), 1–14 (2019)
2. Shafiq, M., et al.: SoftSystem: smart edge computing device selection method for IoT based on soft set technique. Wireless Commun. Mobile Comput. (2020)
3. Kadhim, I.J., et al.: Comprehensive survey of image steganography: techniques, evaluations, and trends in future research. Neurocomputing 335, 299–326 (2019)
4. Wang, X., Feng, L., Zhao, H.: Fast image encryption algorithm based on parallel computing system. Inf. Sci. 486, 340–358 (2019)
5. Amalarethinam, D.G., Geetha, J.S.: Image encryption and decryption in public key cryptography based on MR. In: 2015 International Conference on Computing and Communications Technologies (ICCCCT), pp. 133–138. IEEE (2015)
6. Sumathi, R., Raajan, N.R.: A multilevel distributed image based encryption for full integrity. Multimed. Tools Appl. 79(3), 2161–2183 (2020)
7. Shafiq, M., Yu, X., Bashir, A.K.: A machine learning approach for feature selection network traffic classification using security analysis. J. Supercomput. 74(2), 1–26 (2018)
8. Qin, J., et al.: Coverless image steganography: a survey. IEEE Access 7, 171372–171394 (2019)
9. Qin, C., et al.: An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer. Inf. Sci. 487, 176–192 (2019)
10. Dalal, M., Juneja, M.: Steganography and steganalysis (in digital forensics): a cybersecurity guide. Multimed. Tools Appl. 80(2), 1–49 (2020)
11. Bak, P., et al.: Application of perfectly undetectable network steganography method for malware hidden communication. In: 2018 4th International Conference on Frontiers of Signal Processing (ICFSP), pp. 34–38. IEEE (2018)
12. Shafiq, M., et al.: IoT malicious traffic identification using wrapper-based feature selection mechanisms. Comput. Secur. 94, 101863 (2020)
13. Tao, J., et al.: Towards robust image steganography. IEEE Trans. Circuits Syst. Video Technol. 29(2), 594–600 (2018)
14. Hu, D., et al.: A novel image steganography method via deep convolutional generative adversarial networks. IEEE Access 6, 38303–38314 (2018)
15. Raut, G.G., Chavan, R.: A novel approach for image steganography based on LSB technique. In: Proceedings of the International Conference on Compute and Data Analysis, pp. 167–170 (2017)
16. Muhammad, K., et al.: Image steganography for authenticity of visual contents in social networks. Multimed. Tools Appl. 76(18), 18985–19004 (2017)
17. Artienjew, P., Kislak-Malinowska, A.: Indiscernibility mask key for image steganography. Computers 9(2), 38 (2020)
18. Li, Q., et al.: A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks. IEEE Access 8, 168166–168176 (2020)
19. Mukherjee, S., Sanyal, G.: Image steganography with N-puzzle encryption. Multimed. Tools Appl. 79(39), 29951–29975 (2020)
20. Solak, S., Altnsubmission and encryption method: adaptive LSB + 3. J. Electron. Imaging 28(4), 043025 (2019)
21. Mazarizey, W., Wendrel, S.: Information hiding: challenges for forensic experts. Commun. ACM. 61(1), 86–94 (2017)
22. Kordov, K., Stoyanov, B.: Least significant bit steganography using Hitzel-Zele chaotic map. Int. J. Electron. Telecommun. 63(4) (2017)
23. Kuznetsov, O., et al.: Lightweight stream ciphers for green IT engineering. In: Green IT Engineering: Social, Business and Industrial Applications, pp. 113–137. Springer (2019)
24. Kim, D.H., Lee, H.Y.: Image manipulation detection using convolutional neural network. Int. J. Appl. Eng. Res. 12(21), 11640–11646 (2017)
25. Zhan, Y., et al.: Image forensics based on transfer learning and convolutional neural network. In: Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security, pp. 165–170 (2017)
26. Cavallaro, A., Malekzadeh, M., Shamsabadi, A.S.: Deep learning for privacy in multimedia. In: Proceedings of the 28th ACM International Conference on Multimedia, pp. 4777–4778 (2020)
27. Li, S., et al.: Data hiding in iris image for privacy protection. IETE Tech. Rev. 35(1), 34–41 (2018)
28. Newman, J., et al.: StegoAppDB: a steganography apps forensics image database. Electron. Imaging 2019(5), 536–1 (2019)
29. Zhou, Z., et al.: Introduction to the special issue on deep learning for real-time information hiding and forensics. J. Real Time Image Process. 17(1), 1–5 (2020)
30. Zou, L., et al.: A novel coverless information hiding method based on the average pixel value of the sub-images. Multimed. Tools Appl. 78(7), 7965–7980 (2019)

How to cite this article: Khan, A.A., et al.: IMG-forensics: Multimedia-enabled information hiding investigation using convolutional neural network. IET Image Process. 1–9 (2021). https://doi.org/10.1049/ipr.212272