Hindawi
Scientific Programming
Volume 2022, Article ID 4189148, 7 pages
https://doi.org/10.1155/2022/4189148

*Research Article*

# An Improved Privacy Protection Algorithm for Multimodal Data Fusion

**Z. F. Chen**,[1] **J. J. Shuai**,[1] **F. J. Tian**,[2] **W. Y. Li**,[1] **S. H. Zang**,[1] **and X. Z. Zhang**[1]

[1]*School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China*
[2]*Mandarin Training and Testing Center of Jilin Province, Changchun 130022, China*

Correspondence should be addressed to Z. F. Chen; chenzhanfang@cust.edu.cn

Received 30 May 2022; Revised 8 July 2022; Accepted 25 July 2022; Published 23 August 2022

Academic Editor: Lianhui Li



With the rapid development of Internet technology, the use and sharing of data have brought great opportunities and challenges to mankind. On the one hand, the development of data sharing and analysis technology has promoted the improvement of economic and social benefits. On the other hand, protecting private information has become an urgent issue in the Internet era. In addition, the amount and type of information data are also increasing. At present, most algorithms can only encrypt a single type of small-scale data, which cannot meet the current data environment. Therefore, it is very necessary to study the privacy protection algorithm of multimodal data fusion. To improve the security of privacy protection algorithm, combined with the idea of multimode, this paper combines the improved traditional spatial steganography algorithm LSB matching method and the improved traditional transform domain steganography algorithm DCT with AES encryption algorithm after modifying the S-box and then combines it with image stitching technology, so as to realize a safe and reliable privacy protection algorithm of multimode information fusion. The algorithm completes the hidden communication of private information, which not only ensures that the receiver can accurately recover private information in the process of information transmission but also greatly improves the security of private information transmission.

## 1. Introduction

With the rapid development of Internet technology, the use and sharing of data have brought great opportunities and challenges to mankind. Nowadays, people pay more and more attention to their private information. The college entrance examination registration and voluntary filling system provide services to more than 10 million candidates across the country. These candidates' personal information is stored in the college entrance examination registration and voluntary filling system; the national social security system is more about the pension, medical care, employment, and other information of hundreds of millions of people across the country. The development of data sharing and analysis technology has promoted the improvement of economic and social benefits. At the same time, the protection of private information has become an urgent problem in the Internet era. At present, the amount of information is increasing, and there are more and more types. Most algorithms can only encrypt a single type of small-scale data, which cannot meet the current data environment. Therefore, it is necessary to study the privacy protection algorithm of multimodal data fusion.

In recent years, pin academics have achieved a series of results on traditional modified/embedded information hiding. Literature [1] proposed a data hiding/protection strategy combining PVD (pixel value difference), LSB, and MPE (modification of prediction error) to improve steganographic capacity and resistance to RS steganalysis. The literature [2] uses MSB (most significant bit) to select the best embedding point and combines the AES encryption algorithm to embed the ciphertext in the lowest significant bit of that point. Literature [3] implements a digital watermarking technique based on hybrid multibit multiplication rules by secret key control from the DWT domain.

Meanwhile, the concept of reversible data hiding (RDH) has been proposed from the perspective of whether the original carrier image can be recovered. Reversible data hiding refers to embedding secret information into the "reversible domain" of the original carrier image so that the image can be recovered without distortion after extracting the secret information. This technique is widely used in military, medical, and legal forensic fields. Literature [4] proposes embeddable pixel pairs (EPP, embeddable pixels pairs) as the embedding unit of secret information and achieves reversible information hiding through secret bit extraction and carrier recovery. Although the focus of reversible information hiding is on the lossless recovery of the carrier, the encryption process also inevitably makes modifications to the original carrier.

Zero-hiding techniques guide the change of steganography from embedding to nonembedding. The multilayer partially homomorphic textual information steganography based on zero-hiding proposed in literature [5] achieves a better balance in terms of robustness, security, and capacity. However, in the image domain, zero-hiding follows that although it achieves no modification of the image carrier, it generates other necessary information as the secret key for decoding by the receiver, such as associated documents and secret message extraction files, thus causing additional channel occupation.

At present, the traditional "coding/mapping" approach is more mature, and the evaluation scheme has been established by the academic community in recent years. In [6], the image grid is divided and the image SIFT features are combined with hash sequences to quantize and encode the feature sequences and build an image library, which can be used for indexing. The literature [7] adopts the idea of carrier-free information hiding and uses the brightness features of the material molecular structure for encoding to establish the mapping relationship between binary sequences and image carriers. The literature [8] focuses on image global features, quantization coding the gray gradient coeval matrix to achieve carrier-free information hiding and constructing a high-secure satellite communication model. The classical transformation methods in information hiding are discrete cosine transform (DCT), discrete wavelet transform (DWT) [9], and discrete Fourier transform (DFT) [10]. The literature [11] proposes carrier-free information hiding based on DCT (discrete cosine transform) and LDA (latent Dirichlet allocation, document topic generation model) models.

In summary, information hiding algorithms have been progressing in the process of exploration, and different steganography methods have different focuses on performance evaluation. However, on the issue of "how to hide," many existing steganographic methods always revolve around the three existing frameworks, while combining various technologies to jointly promote the development of information hiding.

Based on the traditional steganography embedding algorithm, this paper improves the spatial domain steganography algorithm and transforms the domain steganography algorithm to improve the embedding capacity and antisteganalysis ability of the algorithm. Combined with image stitching technology, the mapping capacity of the noncarrier information hiding algorithm is improved, and the large capacity noncarrier information hiding algorithm is used to hide the key. Joint information encryption method is to achieve multimodal data fusion privacy protection system. The system improves the diversity and security of the system by using the key control steganography algorithm.

## 2. Multimodal Data Fusion Privacy Protection Algorithm

*2.1. Improved Spatial Domain Steganography Algorithm.* However, the disadvantage of the traditional LSB algorithm is that when the embedded message is large, it takes a long time, and it can only deal with simple stream format files. So, in this paper, based on the traditional LSB matching algorithm, according to the texture characteristics of the image, the texture complex region is selected to embed the private information into the carrier image with complementary embedding rules. The embedding capacity of the traditional LSB matching algorithm is improved. The traditional LSB matching algorithm is to embed secret information into gray images randomly. At present, color images are generally used in network transmission. Therefore, this paper first divides them into RGB layers, selects regions with complex image textures to embed private information, and embeds them into different color layers in different regions of the carrier image in a complementary, so as to improve the embedding capacity and undetectability of the spatial domain steganography algorithm.

*2.1.1. RGB Layered.* The color image has RGB three color channels, and the three-channel component diagram is different. When the secret image is hidden in different layers, it is different from the original carrier image. The secret image is hidden in the image carrier of each layer of $R$, $G$, and $B$. In this paper, the $R$ channel and $G$ channel are used as complementary channels to embed private information, which can achieve better results in this respect and better resists statistical analysis. In this way, embedding private information in two layers can improve the embedding capacity and reduce the change of the statistical characteristics of the original carrier image caused by private information embedding, which improves the capacity and undetectability of information hiding.

*2.1.2. Image Grayscale Cooccurrence Matrix.* The image gray level cooccurrence matrix can be used to describe the texture features of the image, and the ciphertext is embedded into the complex area of the texture features of the image. The effective steganography of the ciphertext is completed by using the redundant space of the image [12].

In this paper, four parameters (energy, entropy, dissimilarity, and correlation) are derived to describe the texture characteristics of the image gray level cooccurrence matrix in image texture analysis.

$$\text{Energy} = \sum_{i=0}^{L-1}\sum_{j=0}^{L-1} P(i,j)^2, \tag{1}$$

$$\text{Entropy} = \sum_{i=0}^{L-1}\sum_{j=0}^{L-1} P(i,j)\log_2 P(i,j), \tag{2}$$

$$\text{Inertia} = \sum_{i=0}^{L-1}\sum_{j=0}^{L-1} |i-j| p(i,j), \tag{3}$$

$$\text{Coherence} = \frac{\sum_{i=0}^{L-1}\sum_{j=0}^{L-1}(i+1)(j+1)p(i,j) - \mu_1\mu_2}{\delta_1\delta_2}. \tag{4}$$

These four features respectively reflect the characteristics of the gray distribution of the image, including uniformity, the thickness of the capacity texture of the carrier image, and the similarity of the elements in the matrix. The matrix is formed by these four features, $T\ (4) = \{\text{Energy, Entropy, Inertia, Coherence}\}$. Then, the embedding region is determined by selecting parameters.

*2.1.3. Embedding of Secret Information.* The spatial domain steganography algorithm first extracts the texturally complex subblocks of the original color carrier image. The ciphertext is divided into two groups and the carrier image subblock texture features are used to obtain the embedding position. A set of ciphertext is embedded in the $R$ channel in +1 form and a set of ciphertext is embedded in the $G$ channel in −1 form, and the channels are combined to obtain a color image containing the cipher.

*2.2. Improved Transform Domain Steganography Algorithm.* Based on the traditional modified message hiding transform domain steganography algorithm, this paper divides the color image into three channels of RGB for embedding the ciphertext to increase the embedding capacity. The ciphertext is grouped into two bits and embedded into the more stable intermediate frequency region after the DCT transform. Because digital images are DCT-transformed, the low and medium frequency signals have the highest energy, but the private information embedded in the low and medium frequency signals can easily be observed directly by the human eye; in the high-frequency part, the energy is low and unstable, so the intermediate frequency region after DCT transform is selected for private information embedding. This region can better meet the imperceptibility and robustness of the steganography algorithm.

*2.3. Large Capacity Carrier-Free Information Hiding Algorithm.* The traditional mapped carrier-free information hiding algorithm has the problem of low steganographic capacity. In this paper, multiple mapped images are reorganized and stitched into one image using image stitching technology to improve the steganographic capacity of the carrier-free information hiding algorithm and realize the secure mapped steganographic writing of keys and some private information.

By using the features of the image for binary encoding, a binary sequence can be derived without any modification to the image. In this way, the image can form a mapping relationship with the corresponding private information. This mapping relationship requires a one-to-one correspondence between the private information and the images in the image library. That is, if the length of the binary sequence of private messages is $n$, the image library must have at least $2^n$ images. The value of $n$ has to be chosen appropriately for the possibility of implementation and the security of mapping hidden information.

The steganographic capacity of carrier-less information mapping is low, and image stitching technology is used to improve the steganographic capacity of the algorithm. Multiple images are similarly spliced to form a complete key image and sent to the receiver. Taking the $2 \times 2$ modes as an example, the splicing combination process is shown in Figure 1.

*2.4. Multimodal Data Fusion Privacy Protection Algorithm Design.* The multimodal data fusion privacy protection algorithm uses two images to steganography the ciphertext (private information encrypted to form the ciphertext) and the key, one using a spatial domain steganography algorithm or a transform domain steganography algorithm to steganography the ciphertext, with the key controlling the choice of the specific algorithm, and the other using a carrier-free information hiding algorithm to steganography the key in a mapped fashion. This design can ensure the safe transmission of private information so that any image cannot be decoded after being illegally intercepted. Even if the two images are intercepted, the interceptor does not know the operation mode of the system and cannot crack the contains secret images.

The information transmitted by the multimodal data fusion steganography system consists of two parts: the ciphered image and the key-mapped image. Due to the long length of the AES encryption key, a $6 \times 6$ stitching mode is used and the private information is encrypted by the message encryption technique (AES encryption algorithm after modifying the S-box), and then the ciphertext is embedded in the chosen ciphertext steganography algorithm, where an improved spatial domain steganography algorithm and a transform domain steganography algorithm can be chosen to form the ciphered image. Keymapping image mainly implements mapped hiding of the key; the key consists of two parts, $\text{key} = \{\text{keychoose, keyencryption}\}$; these two parts are, in order, the ciphertext steganography flag bit and the encryption algorithm key. The coverless information hiding technique uses a $6 \times 6$ pattern to stitch the submap into a complete carrier image to form a key mapping image. After receiving the key image, the receiver splits and then deciphers the type of ciphertext steganography algorithm used and the key of the encryption algorithm, respectively. The effect of the secret image is shown in Figure 2. The cryptographic image and the key mapped


Figure 1: Splicing assembly process.

(a) (b)

Figure 2: (a) Secret images. (b) Keymapping images.

image are transmitted, and then the receiver gets the private information in a specific way.

As shown in Figure 2, after receiving the key-mapped image and the cryptographic image, the receiver needs to first segment the key-mapped image according to the rules to obtain 36 subimages. The subgraphs are decrypted separately in mapped form, and the decrypted results are combined in stitching order to obtain the key for the complete encryption algorithm and to determine the type of steganography algorithm using the first-bit flag bit, with the spatial domain steganography selected if the first bit is 0, and the transform domain steganography is selected if it is 1. The ciphertext is decrypted by the corresponding steganographic algorithm on the cryptographic image, and the ciphertext is decrypted by the encryption algorithm key obtained from the key-mapped image to obtain the plaintext.

The process of implementing the multimodal data fusion privacy protection algorithm is shown in Figure 3, where the private information and the key of the encryption algorithm are first encrypted to obtain the ciphertext. The spatial domain steganography algorithm or transform domain steganography algorithm is selected to embed the ciphertext, and the modified embedding algorithm is selected to embed the ciphertext. The secret key containing the type symbol of the ciphertext steganography algorithm and the information encryption key is obtained. The secret key is mapped by the noncarrier information hiding mapping algorithm, and the encrypted image and the key mapping image are generated.

When decrypting, the key mapping image is first segmented and then decrypted by the carrier-free information hiding algorithm. The codes corresponding to the 36 subgraphs are decoded according to the carrier-free information hiding technique; the codes are combined and processed to obtain the key of the encryption algorithm and the ciphertext steganography algorithm type flag. The cryptographic image is then decrypted according to a determined steganographic algorithm to produce the ciphertext. Finally, based on the previously derived key, the private message is decrypted by an encryption algorithm.

## 3. Algorithm Implementation

*3.1. System Implementation.* The multimodal data fusion privacy protection algorithm consists of several application forms, the core of which is the data fusion steganography. Click on the image fusion steganography, there are two links for the sender and the receiver, and select the sender. There are three inputs on the transmitter side: the plaintext before processing, the encryption key, and the carrier image selection path. One input, the selection of the ciphertext steganography algorithm, is used to implement the selection of the spatial domain steganography algorithm or the transform domain steganography algorithm. There are 3 output items: the encrypted ciphertext, the mapped image 1, and the encrypted image 2. There are six additional function buttons: Encryption, Key Mapping, Browse, Ciphertext Steganography, Save, and Send. A brief description of each function button is given follows (Figure 4):

(1) Encryption: encryption of the input plaintext and a key of a specific length to obtain the ciphertext using the AES encryption algorithm with a modified *S*-box;

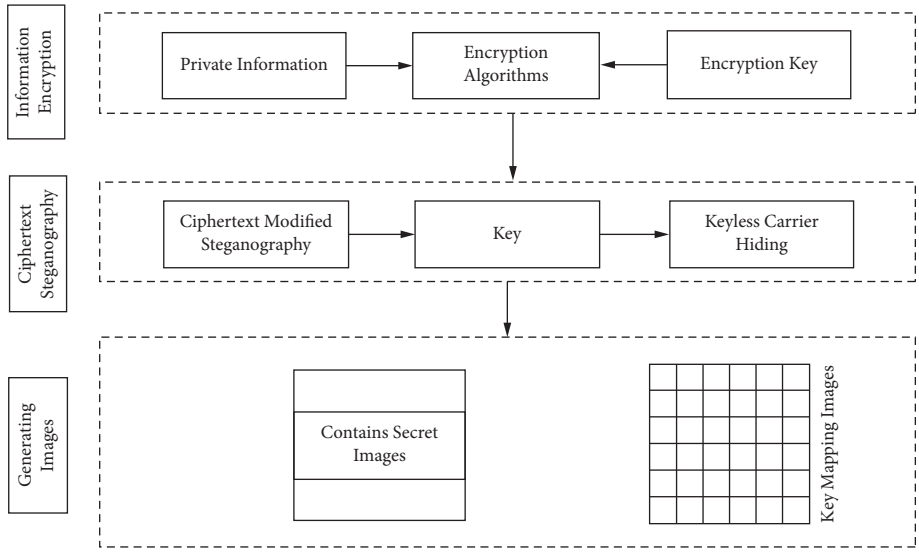


Figure 3: The encryption process of multimodal data fusion privacy protection algorithm.

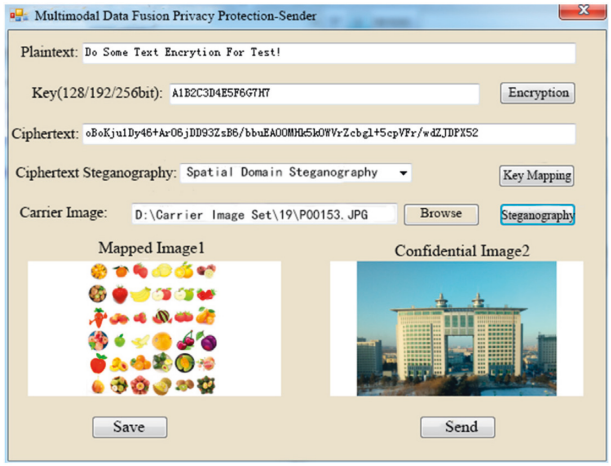


Figure 4: Sender-side steganography-spatial domain steganography.

(2) Key Mapping: based on the chosen ciphertext steganography algorithm and the encryption algorithm key, a carrier-free information hiding mapping steganography is performed to obtain mapped image 1;

(3) Browse: jump to the image selection page and select the appropriate carrier image for ciphertext steganography;

(4) Ciphertext steganography: the ciphertext obtained in (1) is steganographically written to the carrier image in (3) according to the selected ciphertext steganography method, and the sender selects the spatial domain steganography algorithm to complete the steganographic effect as shown in Figure 4;

(5) Save: jump to the image, save the page, and select the save path option to save the mapped image 1 and the encrypted image 2 locally;

(6) Send: jump to the send page, fill in the recipient's details, and transmit two coded images to the sender.

The multimodal data fusion privacy-preserving-receiver side is shown in Figure 5, with a total of one input item being the path selection of the image containing the secret. The three output items are the mapped image 1, the coded image 2, and the plaintext (private message). Five function buttons are included, namely, Browse, Get Mapped Image 1, Get Confidential Image 2, Decrypt, and Clear buttons. A brief description of each function button is given as follows:

(1) Browse: it obtains the path to the folder containing the key-mapped image and the ciphertext steganography image;

(2) Get Mapped Image 1: the system reads the key mapping image in the specified folder and segments the key mapping image, storing the 36 subimages in the order in the program directory;

(3) Obtaining a Confidential Image 2: the system reads the ciphertext steganography image under the specified folder and displays it in the system interface;

(4) Declassify: the subgraph obtained from (2) is decrypted by the carrier-free information hiding algorithm mapping, combined, and processed to obtain the ciphertext steganography flag and the encryption algorithm key, the corresponding steganography decryption algorithm is performed on the carrier image 2 to obtain the ciphertext, and the ciphertext is decrypted according to the AES decryption algorithm after modifying the S-box, resulting in the plaintext, and displayed;

(5) Clear: it clears the cryptographic image selection, the mapped image, the encrypted image, and the plaintext and deletes the split subimage of the key-mapped image stored in the program directory, clears the system cache image, and restores the receiver page to the initial page.

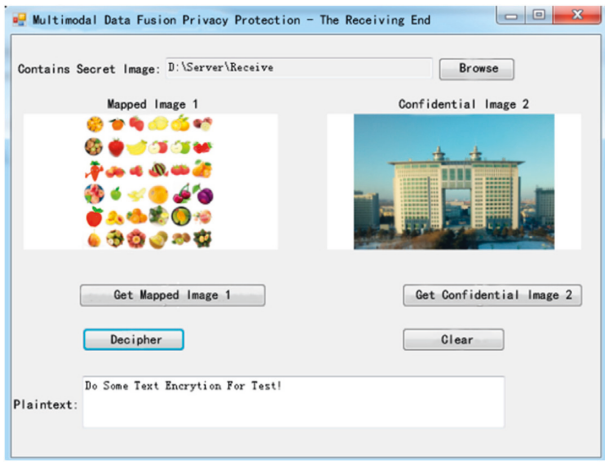


Figure 5: Decryption completion page on the receiving end.

As can be seen from the above, this system implements a multimodal data fusion privacy protection algorithm, which encrypts private information by modifying the AES encryption algorithm after the S-box and completes the steganography of the ciphertext and key after the information hiding algorithm (improved spatial domain steganography, improved transform domain steganography, and carrier-free information hiding algorithm). The receiver decrypts the key and the ciphertext according to the two steganographic images in turn and then performs the message decryption operation to recover the private message accurately.

*3.2. Non-detectability Analysis.* Multimodal data fusion privacy protection algorithms are implemented by three types of algorithms: information encryption algorithms, modified steganography algorithms (improved spatial domain steganography and improved transform domain steganography), and high-capacity carrier-free information hiding algorithms. The proper fusion of these algorithms makes the multimodal data fusion privacy protection algorithm highly secure. The following analysis addresses the undetectability of key-mapped images and ciphertext images in the multimodal data fusion privacy protection algorithm.

The undetectability of the multimodal data fusion privacy protection algorithm is objectively evaluated from the perspective of mathematical-statistical analysis. The key-mapped images before and after steganography are evaluated using root mean square error and peak signal-to-noise ratio, with the root mean square error calculated as shown in equation (5) and the peak signal-to-noise ratio shown in (6).

$$\mathrm{MSE} = \frac{\sum_{x=0}^{N_x} \sum_{y=0}^{N_y - 1} [S'(x,y) - S(x,y)]^2}{N_x \times N_y}, \tag{5}$$

$$\begin{aligned} \mathrm{PSNR} &= 10\lg\left(\frac{(\max S(s,y))^2}{\mathrm{MSE}}\right) \\ &= 20\lg\left(\frac{\max S(s,y)}{\mathrm{MSE}}\right), \end{aligned} \tag{6}$$

Table 1: Test results.

| Spatial domain steganography ratio | Transformation field steganography ratio | JSTEG detection ratio |
|---|---|---|
| 0.1 | 0.1 | 0 |
| 0.2 | 0.2 | 0 |
| 0.3 | 0.3 | 0 |
| 0.4 | 0.4 | 0 |
| 0.5 | 0.5 | 0 |

where S $(x, y)$ is the gray value of the sampled points of the key-mapped images and S $(x, y)$ is the gray value of the sampled points of the stitched original images. The smaller the MSE value, the smaller the image distinction, and similarly, the larger the PSNR value, the smaller the image distinction. The key-mapped images in this paper are not different from the original images, and the root mean square error and peak signal-to-noise ratio are calculated as shown in the following equations:

$$\mathrm{MSE} = 0, \tag{7}$$

$$\mathrm{PSNR} = \infty. \tag{8}$$

Based on the mathematical-statistical analysis, it can be concluded that the key mapping image of the multimodal data fusion privacy protection algorithm is completely undetectable; in other words, none of the existing steganalysis algorithms can detect the key information in the key mapping image.

The JSTEG method was used to detect the embedding rate of cryptographic images and to verify the undetectability of the steganography algorithm. The detection of the $600 \times 400$ pixel cipher laden image was performed using the JSTEG method, which is an information hiding algorithm based on JPEG images, with the steganography ratio incremented from 0.1 to 0.5, and the detection results were obtained as shown in Table 1.

From Table 1, it can be concluded that the detection result of the JSTEG algorithm is 0 for both spatial domain steganography algorithm and transform domain steganography algorithm, JSTEG cannot effectively detect the ciphertext steganography method used in this paper, and ciphertext steganography with multimodal data fusion privacy protection has good effect in resisting dedicated steganography analysis algorithm.

## 4. Conclusions

This paper designs and implements a multimodal data fusion privacy protection algorithm based on image steganography, joint information encryption algorithms, steganography of encrypted ciphertext by two modified embedding steganography algorithms (spatial domain steganography and transform domain steganography), and mapped steganography of key according to the carrier-free information hiding algorithm. The algorithm has proved through experiments to be a great guarantee of the security of private information.

Future attempts can be made to combine it with deep learning of artificial intelligence technology to further improve the efficiency and algorithmic diversity of the algorithm. In the mentioned image fusion encryption, this paper has not considered the fusion in multiple modes, which needs further research.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This work was supported by the Science and Technology Research Program of Jilin Province, China (Nos. 20190201267JC and 20200703003ZP).

## References

[1] M. Hussain, A. W. A. Wahab, N. Javed, and K. H. Jung, "Recursive information hiding scheme through LSB,PVD shift, and MPE," *IETE Technical Review*, vol. 35, no. 1, 2018.

[2] Z. Sultana, F. Jannat, S. S. Saumik, N. Roy, N. K. Datta, and M. N. Islam, "A new approach to hide data in color image using LSB steganography technique," in *Proceedings of the IEEE International Conference on Electrical Information & Communication Technology*, Khulna, Bangladesh, December 2017.

[3] J. B. Wu, X. X. Fei, and N. F. Wang, "Research on image zero hiding algorithm based on chaotic sequence and DCT transform," *Electronic Measurement Technology*, vol. 40, no. 5, pp. 174–179, 2017.

[4] J. L. Wang, X. Sun, and X. Q. Feng, "Adaptive reversible information hiding using pixel permutation," *Chinese Journal of Graphical Graphics*, vol. 23, no. 1, pp. 1–8, 2018.

[5] N. Naqvi, A. T. Abbasi, R. Hussain, M. A. Khan, and B. Ahmad, "Multilayer partially homomorphic encryption text steganography (MLPHE-TS):A zero steganography approach," *Wireless Personal Communications*, vol. 103, 2018.

[6] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," *Intelligent Computing Methodologies*, Springer, vol. 10363, pp. 536–547, Heidelberg, Germany, 2017.

[7] Y. Cao, Z. Zhou, X. Sun, and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Computers, Materials & Continua*, vol. 54, no. 2, pp. 197–207, 2018.

[8] J. B. Wu, Y. W. Liu, Z. W. Kang, S. RahbarJia, and Y. Jia, "A coverless information hiding algorithm based on grayscale gradient Co-occurrence matrix," *IETE Technical Review*, vol. 35, no. 1, pp. 23–33, 2018.

[9] S. Roy and A. K. Pal, "A hybrid domain color image watermarking based on DWT-SVD," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 2, pp. 201–217, 2019.

[10] X. T. Zhang, Q. T. Su, Z. H. Yuvan, and D. Liu, "An efficient blind color image watermarking algorithm in spatial domain combining discrete Fourier transform," *Optik-International Journal for Light and Electron Optics*, vol. 219, no. 2, Article ID 165272, 2020.

[11] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223–3238, 2018.

[12] T. D. Denemark, M. Boroumand, and J. Fridrich, "Steganalysis features for content-adaptive JPEG stegano- graphy," *IEEE Transactions on Information Forensics and Security*, vol. 11, 2016.