IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 August 2022, accepted 21 August 2022, date of publication 31 August 2022, date of current version 22 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3203173

TOPICAL REVIEW

Systematic Survey on Visually Meaningful Image Encryption Techniques

VARSHA HIMTHANI[1], VIJAYPAL SINGH DHAKA[1], MANJIT KAUR[2], (Senior Member, IEEE), DILBAG SINGH[2], (Senior Member, IEEE), AND HEUNG-NO LEE[2], (Senior Member, IEEE)

[1]Computer and Communication Engineering, Manipal University Jaipur, Jaipur, Rajasthan 303007, India
[2]School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea

Corresponding author: Heung-No Lee (heungno@gist.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) Grant through the Korean Government (MSIP) under Grant NRF-2021R1A2B5B03002118; and in part by the Ministry of Science and ICT (MSIT), South Korea, through the Information Technology Research Center (ITRC) Support Program supervised by the Institute of Information and Communications Technology Planning and Evaluation (IITP) under Grant IITP-2021-0-01835.

ABSTRACT Due to advancements in technology, digital images are widely used in various applications like medical field, military communication, remote sensing, etc. These images may contain sensitive and confidential information. Therefore, images are required to be protected from unauthorized access. Many image protection techniques have been proposed in past years. The most common technique to protect the images is encryption. In this technique, a secret key and an encryption algorithm are used to change the plain image into an encrypted image. The encrypted image looks like a noisy image and can easily attract the attacker's attention. If an image gets captured and stacked, sensitive information can be revealed. In this regard, Visually Meaningful Encrypted Image (VMEI) technique is developed, which initially encrypts the original image and then hides it into a reference image. The final encrypted image looks like a normal image. Hence, the VMEI technique provides more security as compared to simple image encryption techniques. Therefore, a systematic survey of existing VMEI techniques is presented in this paper. The VMEI techniques are divided into different categories based on their characteristics. Moreover, this paper elaborates and investigates the improvements and analyses performed on VMEI techniques based on various evaluation parameters. These evaluation parameters are divided into different categories such as security attacks, encryption key attacks, quality analysis, and noise attacks. Finally, this paper discusses the potential applications and future challenges of VMEI techniques.

INDEX TERMS Embedding, encryption, information security, visually meaningful image encryption, attacker, attacks.

I. INTRODUCTION

Nowadays, online information storage and transmission facilities are provided by many vendors to organizations, businesses, and other consumers. It is a better alternative to traditional information storage and transmission methods because of fast access time, easy sharing, and many other advantages. Information may be in the form of a text document, digital image, audio, and video [1]. Information security is essential to keep it secure from unauthorized access, release, disclosure, alteration, copy, or damage, as it is an asset for any organization or business [2].

A digital image is one of the forms of data that is used to store pictorial information and to communicate secret data over the computer network [3]. Image encryption is a cryptographic method to encode a secret image in such a way that the unauthorized user can't understand it [4]. In recent years, various image encryption algorithms are developed. These algorithms are mainly based on spatial and frequency domains. In the spatial domain, algorithms usually jumble the pixels through matrix transformation and extinguish the pixel's correlation of the secret image. In the

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Liu.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

frequency domain, the encryption algorithm transforms the spatial secret image into the frequency domain first, then modify the coefficients according to some rules, and then converts the coefficients to the spatial domain [5]. When these algorithms are applied to a secret image then the transformed encrypted image is look-like completely noisy (see Figures 1 (a) and (b)). These noise-like images indicate that confidential information is hidden.

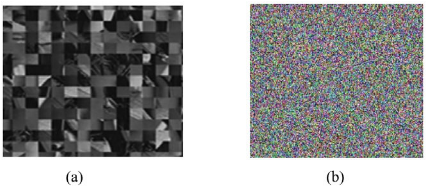


FIGURE 1. Encrypted images: a) Texture-like and b) Noise-like.

Hence, the attackers can easily recognize the target image. This issue has been resolved by researchers by proposing the concept of a Visually Meaningful Encrypted Image (VMEI) [5]. In this, the final encrypted image will not be noise-like by the use of steganography.

Steganography is the other data security technique in the field of network security. In this technique, the secret image is embedded in some other cover media like image, audio, or video, *etc.* [6], [7], [8], [9]. However, there are some steganalysis techniques [10], that can extract the secret hidden image from the cover media. Hence, to provide additional security to the highly confidential data, VMEI techniques are proposed. The advantage of the VMEI technique is that, even though the secret data is extracted by the steganalysis tool, the extracted data will be in the form of noise-like image and the attacker will not get the secret image through steganalysis only. The disadvantage of the VMEI techniques is that the computational burden is high because two security steps are performed.

The basic idea of VMEI constitutes two steps: in the first step, a secret image is transformed into a noise-like or texture-like encrypted image using any existing image encryption algorithm [5]. In the second step, an encrypted image is embedded into a reference image using some image fusion method. So, the final encrypted image looks like a reference image. Therefore, in VMEI, the final encrypted could not be easily distinguishable from normal images. The process of generating visually meaningful encrypted images is illustrated in Figure 2.

In the first phase, the chaotic map can be used to encrypt the images by obtaining the random secret keys efficiently [11], [12], [13], [14]. Permutation and diffusion operators can be used to encrypt the images using secret keys obtained from chaotic maps. A simple 1D chaotic map can obtain secret keys as follows:

$$cs_{n+1} = C \times \mathrm{CS}_{n+1} \times (1 - \mathrm{CS}_n) \tag{1}$$

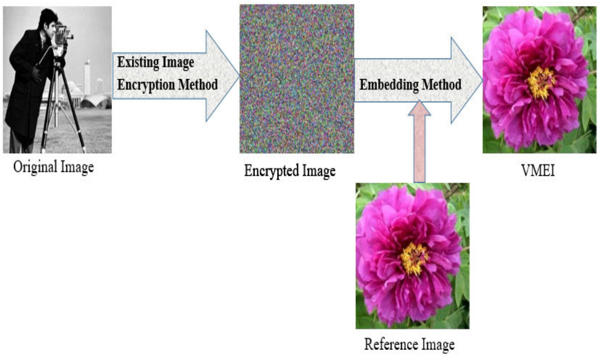


FIGURE 2. Block diagram of VMEI.

Here, C is the control parameter, with value lies in between 0 to 4. cs_0 and cs_n represents the initial and generated random value of chaotic map respectively [11]. In Algorithm 1, the procedure to encrypt a M × N color image is illustrated.

To represent a grayscale image, one byte for each pixel is required. One byte can store 0 to 255 values that cover all possible shades of a gray color. A grayscale image is denoted as a two-dimensional array of bytes in memory and this array is called a channel. A grayscale image has only one channel. For the color image (using RGB color space), 3 bytes are required for each, one byte for each color. Hence, a color image has three channels. The encryption process is required for three matrices in the case of color image whereas, there is a single matrix to be encrypted in a grayscale image. Hence, the encryption burden is high for the color image as compared to the grayscale image. However, the color image encryption method could be complex because there are three matrices that can be manipulated with each other that provide high security. Moreover, we can use the same algorithm to encrypt the color image that is designed for encrypting a grayscale image by applying the same procedure to all three channels of the color image that is designed for one channel of a grayscale image.

In Algorithm 1, a secret color image I is converted into one dimensional matrix of size $M \times 3N$. The initial values for the chaotic map and control parameter are the secret keys. The generated chaotic map is sorted in ascending order to get the sorted sequence $\mathrm{S}^{'}$. Finally, to get the encrypted noise-like image, the one dimensional I matrix is permuted according to $\mathrm{CS}^{'}$ [12]. Algorithm 1 depicts the basic example of chaotic map-based encryption. Similarly, the other hyper chaotic map-based encryption techniques are implemented [13], [14].

The second phase is embedding an encrypted image I' into reference image R. This embedding is performed in frequency domain through Discrete wavelet transform (DWT) [15], [16], [17]. In this, the reference image is decomposed into four matrices denoted as C_{a} (approximation matrix), C_{h}, C_v and C_d [5]. The parameter set P is used to define the filters used in DWT. The DWT is defined as the following equation-

$$\mathrm{VMEI} = \mathrm{DWT}\left(I', R, P\right) \tag{2}$$

```
Algorithm 1 Pre-Encryption
  Input:   Color image $I$ of size M × N.
  Output:  Encrypted Image $I'$
  Step 1:  The $I$ is converted into one dimensional $I = \{p_0, p_1, \ldots\ldots p_{\mathrm{M}\times 3\mathrm{N}}\}$matrix of size $M \times 3N$
  Step 2:  The initial values $cs_0$ and control parameter $C$ are used as secret keys. The chaotic sequence CS is obtained using these keys
  Step 3:  Sort the chaotic sequence to obtain $\mathrm{CS}' = \left\{\mathrm{cs}_0^{'}, \mathrm{cs}_1^{'}, \ldots\ldots .\mathrm{cs}_{M\times 3N}^{'}\right\}$
  Step 4:  $I$ pixels are permuted according to $\mathrm{CS}^{'}$ and $I'$ is obtained as- $I'(i) = I\left(\mathrm{CS}^{'}(i)\right)$
  Step 5:  The obtained encrypted image $I'$ is noise-like
```

```
Algorithm 2 Embedding
  Input:   Encrypted Image $I'$ of size $M \times N$, Reference image $R$ of size $2M \times 2N$, and parameter $P$
  Output:  $VMEI$
  Step 1:  Decompose $R$ into four matrices $C_{\mathrm{a}}$, $C_{\mathrm{h}}$, $C_v$, and $C_d$
  Step 2:  for $x = 1$ to $M$ do
               for $y = 1$ to $N$ do
                   $C_v(x, y) = floor[\frac{I'(\mathrm{x,y})}{10}]$
                   $C_d(x, y) = I'(\mathrm{x, y})\ (\mathrm{mod}10)$
               End for
           End for
  Step 3:  Apply inverse DWT to $C_{\mathrm{a}}$, $C_{\mathrm{h}}$, $C_v$, and $C_d$
  Step 4:  VMEI of size $2M \times 2N$ i.e., Embedded $I'$ in $R$
```

Algorithm 2 illustrates the example of the embedding procedure through DWT [5]. In this, firstly the reference image is decomposed into four subbands of low and high frequencies. After that, the embedding process is applied on low-high and high-high subbands as given in step 2. Finally, after performing embedding, the inverse DWT is applied to get the VMEI [5].

A. RESEARCH GOALS

The motivation behind this survey is to explore the various VMEI techniques and observe their characteristics. The comparative analyses are also performed based on various performance parameters. Moreover, the study comprises the future research directions in VMEI. To the best of our knowledge, this is the first explicit survey performed on the available VMEI techniques. The pinpoints of this study are focused on the following research questions:

RQ 1: How VMEI technique improves image security?

Encrypted images are visually scribbled, which attracts the attacker's attention. VMEI technique is used to produce a meaningful image in two stages of encryption by which image security is increased.

RQ.2: What are the various techniques for generating VMEI? This paper discussed various existing methodologies to generate VMEI. The comparisons between the existing techniques are also drawn with respect to various factors such as security, visual quality, VMEI size, etc.

RQ. 3: What are the challenges of VMEI techniques? In this paper, various problems associated with the existing VMEI techniques are examined. The possible solutions to these problems are also discussed.

To accomplish the aim of answering the research questions, the study comprises databases of ACM, ScienceDirect, IEEE, SpringerLink, and Google Scholar. These databases are used to search and retrieve the published works on the VMEI techniques. Figure 3 shows the number of research papers reported over the last five years, while Figure 4 shows the flowchart of the selection of articles for conducting a systematic survey. The keyword used is visually meaningful image encryption and the published articles' year range is taken from 2015 to 2022.

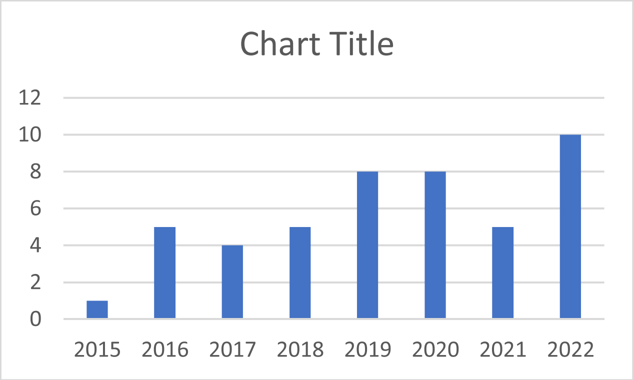


FIGURE 3. Number of studies published on VMEI techniques over years.

Based on this keyword entered in the above-mentioned databases, a total of 22878 articles were found. By screening duplicate articles and based on the title and abstract of the articles, 22658 were sorted out. After the detailed evaluation, 228 articles were found irrelevant. The total number of included articles is 78. Out of the 38 articles are VMEI specific and included in the survey.

B. CONTRIBUTIONS

The key contributions of this paper are:

1) **Comprehensive analytical discussion on the potential of existing VMEI techniques:** The encryption and embedding techniques used in existing VMEI techniques are critically analyzed. Further, the existing techniques are categorized according to their potential.
2) **Comparative assessment of VMEI techniques based on performance parameters:** A detailed comparison and analysis of VMEI techniques are carried out based on various security and image quality measures.
3) **Critical survey on the implementation of VMEI techniques:**A detailed survey of various applications of VMEI techniques is presented with their suitability in different implementation areas.
4) **Recommendations for future research challenges and opportunities:** Recommendations for promising future research areas along with challenges and

research opportunities are presented in the realm of this survey.

The remaining sections of the paper are as follows: the various existing VMEI techniques are presented in Section 2. In Section 3, the performance measures of VMEI are explained. The applications of VMEI are presented in Section 4. The future research challenges and concluding remarks are presented in Section 5 and Section 6, respectively.

II. VISUAL MEANINGFUL ENCRYPTION IMAGE TECHNIQUES

The VMEI concept was proposed to protect the secret image with additional security from attackers [5]. The first time, Bao and Zhou [5] implemented this concept to transmute a secret image into a VMEI. This technique followed two steps such as encryption and embedding. In the first step of encryption, the existing permutation and substitution method were used and in the second step, an encrypted image was implanted in a cover image through Discrete wavelet transform (DWT). After that, various improvements have been suggested by researchers in the field of VMEI. These improvements are broadly categorized based on the improvement in embedding technique, compressive-sensing-based techniques, and improvement in encryption technique (see Figure 5).

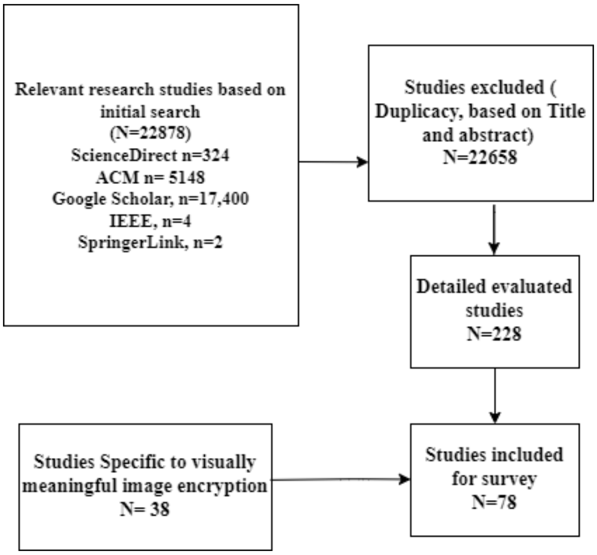

Relevant research studies based on initial search
(N=22878)
ScienceDirect n=324
ACM n= 5148
Google Scholar, n=17,400
IEEE, n=4
SpringerLink, n=2
Studies excluded (Duplicacy, based on Title and abstract)
N=22658
Detailed evaluated studies
N=228
Studies Specific to visually meaningful image encryption
N= 38
Studies included for survey
N=78

FIGURE 4. Flowchart for conducting the systematic survey on VMEI techniques.

The classification of the techniques is divided based on the main contribution of the reviewed technique. The techniques that focus to improve the embedding method, come into the "improvement in embedding technique" category, and the techniques with the main focus to improve the encryption method and making it complex can come in the "improvement in encryption technique" category. The techniques that reduce the VMEI size, come in the "compressive-sensing-based techniques" category.

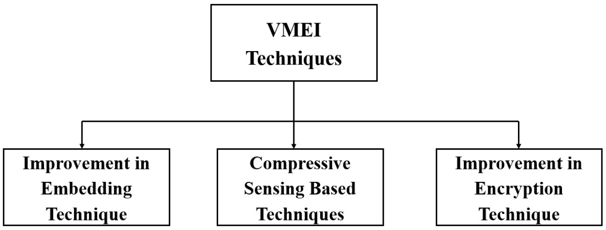

VMEI Techniques
Improvement in Embedding Technique
Compressive Sensing Based Techniques
Improvement in Encryption Technique

FIGURE 5. Categorization of VMEI techniques.

A. IMPROVEMENT IN THE EMBEDDING TECHNIQUE

The bad visual quality of VMEI attracts the attacker and represents the sign of encryption. Some researchers investigated the methods to improve the visual quality of VMEI by improving the embedding technique. Kanso and Ghebleh [18] improved the quality of VMEI and image security as compared to [5]. In this, a 3D chaotic map was used for encryption in the first phase and in the second phase, a 2D Lifting Wavelet Transform (LWT) was used to generate high quality VMEI. The 3D chaotic map was utilized to increase the image security, as these maps are highly sensitive to initial conditions and generate pseudorandom numbers [19]. LWT is an improved implementation of DWT as it is fast in computation, requires less memory, and produces a better-quality recovered image. In DWT, the wavelet coefficients are rounded off to the whole number, so the lossless recovery is not possible [20].

Manikandan and Masilamani [21] proposed improvement in the embedding technique by using DWT and Arnold transform. A reference image was transformed into LL, LH, HL, and HH sub-bands using DWT. An original image was encrypted using an efficient algorithm and decomposed into two matrices. Then, the Arnold transform was applied to each matrix and put into LH and HH sub-bands of the reference image. To determine the periodicity of the Arnold transforms, the additional recovery image information was embedded in the LL sub-band using the conventional LSB data hiding technique. Arnold transform is based on the image scrambling method. In this method, pixels are scrambled by the iterative encoding process. The number of iterations is used as an encryption key to recover the image [22].

Yang *et al.* [23] used discrete quantum walks for the key generation. This key is used for image encryption. An encrypted image is divided into three parts using DWT and embedded into the reference image. The implementation of a quantum walks-based algorithm enhanced the VMEI texture. Yang *et al.* [24] presented a method in which the original image was encrypted using Qi hyper-chaotic system. Block based discrete cosine transform (DCT) was applied to get the coefficient matrix. After that, singular value decomposition (SVD) was applied to each DCT coefficient matrix. This singular value was then embedded into the reference image. A color reference image was converted from RGB to YCbCr color space. DWT was performed on both Cb and Cr. Then, block DCT was used to embed the data into a reference

TABLE 1. Summarizes vmei techniques with improvement in embedding technique.

Ref. No.	Encryption Technique	Embedding Technique	Advantages of the Embedding Technique	Improvements	Challenges
[18]	3D Chaotic map	2D LWT	Low computation cost and better-quality images as compared to DWT	VMEI quality, high security, LWTs are fast and requires lesser memory	VMEI size, visual quality of the reconstructed image
[21]	Permutation and substitution	DWT, Arnold Transform	High compression ratio as compared to DCT; high payload capacity as compared to LSB techniques	VMEI quality	Security, visual quality of reconstructed image
[23]	Discrete quantum walks	DWT	High compression ratio as compared to DCT; high payload capacity as compared to LSB techniques	VMEI quality, security	VMEI size, visual quality of reconstructed image
[24]	Hyper Chaotic map	SVD, DCT	SVD provides extra security against various attacks, DCT provides better performance than LSB method	VMEI quality, security	VMEI size, visual quality of reconstructed image
[25]	Any Existing Encryption technique	Sparse representation coefficients using dictionary	High payload capacity, high security than LSB methods	VMEI quality, Payload capacity	Security, noise resistance, visual quality of reconstructed image
[26]	Any Existing Encryption technique	IWT, 2^k correction method	Low computation cost, better PSNR as compare to DWT, 2^k correction method provides better imperceptibility	VMEI quality, computation speed	Security, VMEI size, visual quality of reconstructed image
[27]	S-Box	2D integer DWT and a substitution box.	Low computation cost, better PSNR as compare to DWT.	VMEI quality, Payload capacity	visual quality of reconstructed image
[28]	RSA Algorithm, Chaotic map	DWT, Schur decomposition	High compression ratio as compared to DCT; high payload capacity as compared to LSB techniques, Schur decomposition provides extra security against various attacks and faster than SVD	VMEI quality, resist against chosen and known plaintext attacks	VMEI size, visual quality of reconstructed image, computation speed
[29]	Any Existing Encryption technique	IWT (Dynamic), 2^k correction method	Low computation cost, better PSNR as compare to DWT.	VMEI quality, Payload capacity, speed	visual quality of reconstructed image
[30]	Chaotic map (salient regions encryption)	DWT	High compression ratio as compared to DCT; high payload capacity as compared to LSB techniques	VMEI quality, Speed	visual quality of reconstructed image
[31]	Chaotic map, DNA (salient regions encryption)	DWT	High compression ratio as compared to DCT; high payload capacity as compared to LSB techniques	VMEI quality, Speed	visual quality of reconstructed image

image. This method contributed to the improvement of VMEI quality.

Li *et al.* [25] presented a compressive-sensing-based data hiding method in which a sparse representation of a reference image was generated using a dictionary (such as a DCT dictionary, wavelet dictionary, etc.). The sparse representation of a reference image was used to hide the encrypted image. Tuncer *et al.* [26] proposed a method in which the encrypted image was divided into Least Significant Bit (LSB) and Most Significant Bit (MSB) and embedded by k least significant bits and 2^k correction method using integer DWT. Armijo *et al.* [27] performed the embedding phase using the 2D integer haar wavelet transform and a substitution box. In [28], chaotic maps are used for encryption and initial values are produced by the RSA algorithm. Schur decomposition was applied to the encrypted image and embedded through DWT. Yang *et al.* [29] proposed a universal embedding model based VMEI technique. In this, a secret image was encrypted by using traditional encryption and dynamically embedded through IWT.

Some authors presented salient regions encryption based VMEI techniques [30], [31]. The salient regions of an image contain useful information. Therefore, the detection and encryption of these regions instead of the full image reduce the computational complexity. In [30], the salient features were detected and encrypted using a parametric switching chaotic system-based image encryption algorithm. Sun *et al.* [31] presented a method in which salient regions were encrypted using a chaotic system and Deoxyribonucleic Acid (DNA) coding. In both the methods [30] and [31], DWT was used for embedding the encrypted image into a reference image. Advantages of the DNA include enormous storage, massive parallelism, very low power consumption, and high speed [32]. However, the implementation of the DNA method requires expensive instruments and bio-molecular laboratories [32].

Table 1 depicts the summary of the VMEI techniques which have improved the embedding method. It represents the method of encryption and embedding used in the technique. It also shows what has improved and is still a challenge in the respected technique.

B. COMPRESSIVE SENSING-BASED TECHNIQUES

In [5], the size of VMEI became double as compared to the original image. From the size, the attackers can easily guess that some confidential information is hidden inside the image. The transmission overhead increases as the size doubles as compared to the original secret image. Therefore, it is necessary to reduce the size of VMEI. Various compressive sensing-based methods have been proposed by researchers to resolve this issue. Compressive sensing is a digital image compression technique that can simultaneously perform encryption by considering the measurement matrix as the shared secret key.

TABLE 2. Compressive sensing based VMEI techniques.

Reference number	The first phase (Encryption)		Second phase	Size of the image (M Rows * N columns)	
	Pixel jumbling for Sparse Representation	Measurement Matrix Generation	Embedding	Original image	VMEI
[35]	ZZ	3D cat map	Dynamic LSB	M*N	M*N
[36]	DWT, ZZ	Chaotic map	DWT	N*N	N/2*N/2
[37]	DWT, ZZ SHA-256	Chaotic map	DWT	M*N	M*N
[38]	ZZ	Chaotic map	Integer wavelet transform (IWT)	N*N	N*N
[39]	DWT, ZZ	Chaotic map	IWT	N*N	N*N
[40]	DWT, 2D chaotic map	3D cat map	Block Replacement	N*N	M*N(M<N)
[41]	DWT, ZZ	Chaotic map	DWT, SVD	N*N	2M*2N
[42]	DWT, chaotic map, SHA 256	4D chaotic map, SVD	IWT	M*N	M/2*N/2 (Color Image) M*N (Gray Image)
[43]	DWT, ZZ	Chaotic map	DWT, DCT	M*N	2M*2N
[44]	DWT, Arnold transformation	Chaotic map, STP	2D DWT	N*N	2N*2N
[45]	DWT	Chaotic map	2D LWT, DCT	M*N (Multiple images)	M*N
[46]	DWT, 4D hyper chaos, Arnold confusion	4D Chaotic map	Slant transform based embedding	M*N	M*N
[47]	Separable wavelet transform, 2D Cat map	Chaotic map	Matrix encoding	M*N	4M *4N

There are mainly three steps followed in compressive sensing. First is the sparse representation of the matrix, the second is measurement matrix generation which acts as an encryption key, and the third is quantification or sparse recovery process [33], which is done by converting the range of values to a single value (see Figure 6). However, the measurement matrix used in compressive sensing endures the problems like storage and memory requirements and calculations.

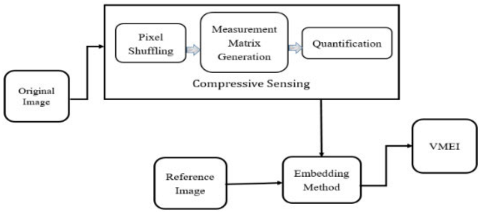


FIGURE 6. Compressive sensing-based VMEI.

Table 2 represents the compressive sensing based on VMEI techniques. In these methods, first pixel shuffling like zigzag confusion (ZZ) [34], etc. is applied to the image to generate a sparse representation, and secondly, different types of chaotic methods are applied to generate the measurement matrix [35], [36], [37], [38], [39], [40], [41], [42], [43], [44]. The pixel jumbling and measurement matrix generation methods used in the techniques [35], [36], [37], [38], [39], [40], [41], [42], [43], [44] are given in Table 2. The key advantage of implementing compressive sensing is to reduce the size of the VMEI. In [36] and [42] it was reduced to half compared to the original image. Whereas VMEI size was the same as the original secret image in [35], [37], [38], [39], [45], and [46]. However, in [43] and [44] VMEI size was not reduced and doubled as compared to the original image. In [44] the VMEI size was increased to maintain the VMEI quality. To increase image security in [36], [37], [39], [40], [41], [42] [43], and [45], DWT was applied before pixel shuffle, that is, compressive sensing in the frequency domain.

A secret image is then embedded into a reference image using different methods to generate VMEI as given in Table 2. Using the compression method, the size of the VMEI can be reduced. The comparison of the size of the original image and VMEI is shown in Table 2. Figure 6 shows the process of compression sensing based on VMEI techniques.

Wen *et al.* [44] presented a VMEI method in which improved compressive sensing is used based on Semi Tensor Product (STP). DWT and Arnold transformation are used to shuffle the pixels of the original image. Then, the measurement matrices obtained are compressed by applying STP. Compressive sensing introduced with STP would reduce the size of the measurement matrix, saving storage and simplifying matrix operations. In [45], multiple images are encrypted, combined, and then embedded in a reference image.

To increase the computational speed parallel [46], [47] and 2D compressive sensing [48] techniques are implemented.

C. IMPROVEMENT IN ENCRYPTION TECHNIQUE

Complex encryption methods are developed to increase the security of the images. Abbasi *et al.* [49] used an intertwining logistic chaotic map to generate random sequences. The original image was permuted row-wise and then column-wise using these sequences. Bitwise XOR was applied to the image pixels with a random matrix. After that, a Gray S-box substitution was performed to get the final encrypted image.

LSB and MSB of the encrypted image were separated and embedded into a reference image using LWT. Khan *et al.* [50] presented a method in which DNA was used for key generation. An image was encrypted by shuffling rows and columns using the quantum chaotic map. Thereafter, a scribbled encrypted image was implanted into a reference image using DWT.

Abood [51] proposed a method in which pixel shuffling and RC4 encryption algorithms were used to encrypt the grayscale image. Hash-LSB steganography was used to embed the encrypted image in the reference image.

Singh and Singh [52] presented a method that encrypted the multiple images and embed into one reference image. This method took multiple color images as input and encrypts them using a logistic chaotic system and elliptic curve. Multiple encrypted images were embedded in the insignificant real data of scrambled color reference images using Arnold transform. Vanamala and Nandur [53] used a genetic algorithm with chaotic maps to encrypt the images. Embedding was performed using DWT.

Pan *et al.* [54] presented a double encryption method that scrambled and diffused the original image using 2D-LASM, modulus operation, and left-shifted in cycles to get the encrypted image. A reference image was also scrambled and diffused. The encrypted image was embedded into the encrypted reference image by using LWT and QR decomposition. The final encrypted image was visually noise-like. If it is identified by an attacker, then VMEI is obtained. Therefore, an attacker cannot recognize that one more encryption stage would be there. Dai *et al.* [55] proposed a VMEI technique for medical image encryption. The original image was confused and diffused using a logistic chaotic map and XOR operation to get the encrypted image. Then, it was embedded into a reference image. Yang *et al.* [56] suggested new VMEI techniques, in this, the secret image is decomposed into four matrices and these matrices are embedded into the subbands of the reference image in the IWT domain with the least significant bit replacement. Table 3 depicts the summary of the VMEI techniques which have improved the VMEI security by improving the encryption technique.

D. RECENT ADVANCEMENTS IN VMEI TECHNIQUES

In recent advancements, some new VMEI techniques are proposed [57], [58], [59], [60], [61]. Huang *et al.* propose a VMEI technique that used digital signatures to provide authenticity and confidentiality. LSB method is used to embed the signature on the encrypted image and LWT is used to generate a VMEI [57]. Abdelfattah *et al.* presented a VMEI technique based on the gyrator transform and the Henon chaotic map. In this method, the optical encryption technique exploits the polarization degree of freedom that provides high security and the proposed method obtains the same size VMEI as the secret image [58]. In recent literature, some compressive sensing based methods are proposed [59], [60]. Huang *et al.* propose a VMEI technique based on asymmetric image encryption and embedding based on SHA-3 and compressive sensing. In this technique, the secret image is divided into blocks. The blocks are scrambled and merged then it is quantized and scrambled again to provide high security [59]. Wang *et al.* presented a VMEI technique based on compressive sensing, 2D DWT, and SVD [60]. Yang *et al.* presented a VMEI technique based on adaptive 2D compressive sensing and chaotic map. The chaotic map is used to generate the measurement matrix and the scrambling sequence for encryption and embedding is performed by the dynamic LSB method based on 2^K correction [61].

TABLE 3. Summarizes VMEI Techniques with improvement in encryption technique.

Ref. No.	Encryption Technique	Embedding Technique	Comments
[49]	Chaotic map, Bitwise XOR, S-box	LWT	high security, resist against noise and data loss attack
[50]	DNA, Quantum chaotic map	DWT	high security, resist against sensitivity attack, brute force attack, statistical attack, cropping attack
[51]	RC4	Hash-LSB	Security, VMEI quality
[52]	Chaotic map, Elliptic curve	Arnold Transform	high security, multiple images are taken as input.
[53]	Genetic algorithm, Chaotic map	DWT	high security, resist against statistical attacks, differential attacks
[54]	Chaotic map, Modulus operation	LWT, QR decomposition,	high security, used encrypted reference image
[55]	Chaotic map	XOR operation	used in medical image security
[56]	Chaotic map, Matrix decomposition	IWT (Dynamic), 2^k correction method	Security, visual quality of VMEIs, robustness, and time efficiency

III. PERFORMANCE EVALUATION PARAMETERS OF VARIOUS VMEI TECHNIQUES

This section represents the various performance parameters to evaluate the different VMEI techniques. These parameters are categorized in such a way that the different aspects such as security, quality, and other attacks of VMEI techniques can be assessed.

A. EVALUATION BASED ON SECURITY PARAMETERS

The primary concern of VMEI techniques is to generate secure encrypted images. The security level can be analyzed by different parameters and these parameters are defined as follows:

1) CORRELATIONAL COEFFICIENT ANALYSIS

The degree of similarity between two contiguous pixels of the image is evaluated using Correlation Coefficient Analysis (CCA). It should be low, so that value of the neighbor pixel cannot be estimated easily [62]. The correlation between two adjacent pixel values x and y of an image can be calculated as-

$$\text{CCA} = \frac{\text{covariance between } x \text{ and } y}{\text{STD of } x \times \text{STD of } y} \tag{3}$$

TABLE 4. Evaluation based on security parameters.

Reference Number	CCA	HA	IEA
[5]	×	✓	×
[18]	×	✓	×
[23]	0.0035	✓	7.9972
[30]	0.9120	✓	×
[31]	0.0232	✓	7.9994
[35]	0.9993	✓	×
[36]	0.9917	×	×
[38]	0.9229	✓	7.2451
[40]	×	✓	7.3836
[41]	×	✓	×
[42]	0.0045	×	7.9986
[43]	0.9982	✓	×
[44]	0.7139	✓	7.9533
[49]	0.0104	×	×
[50]	0.0220	✓	7.9883
[51]	×	✓	×
[53]	0.0573	×	×
[54]	×	✓	×
[55]	×	✓	×

Here, STD stands for standard deviation, which can be calculated as

$$\text{STD of } x = \frac{1}{n}\sum\nolimits_{i=1}^{n}(x_i - M(x))^2 \tag{4}$$

Here, n is the total number of selected adjacent pixels and M represents the mean value of x. Standard deviation of y can be calculated by replacing y in the place of x in (2). Covariance between x and y is calculated as

$$\text{Covariance} = \frac{1}{n}\sum\nolimits_{i=1}^{n}(x_i - M(x))(y_i - M(y)) \tag{5}$$

Table 4 and Figure 7 show the CCA values for different methods. The CCA is calculated between the original and the encrypted images. These values represent the average of CCA calculated for different considered images in methods [23], [36], [50], [53]. In some methods, CCA is calculated in three directions of the image (i.e., horizontal, vertical, diagonal). These values are also taken as average of all three direction CCA values [31], [38], [42], [44], [49], [50]. Figure 7 shows that [23], [42], and [49] has the lowest correlation.

2) HISTOGRAM ANALYSIS

A histogram of an image reflects the distribution of pixel values. It is the graph that shows pixels' frequencies. The histogram of a normal image is random, but it should be uniform for an encrypted image [31]. As the uniform distribution of pixel values is ideal for an encrypted image to repel statistical attacks.

Table 4 shows that Histogram Analysis (HA) is performed to show the effectiveness of the encryption algorithms. There is a minor change in the VMEI histogram and histogram of corresponding reference image [5], [18], [30], [35], [38], [40], [41], [43], [44], [50], [54], [55]. The plotted histogram for the encrypted image is uniform in methods [5], [23], [31], [50], [51], [54], [55].

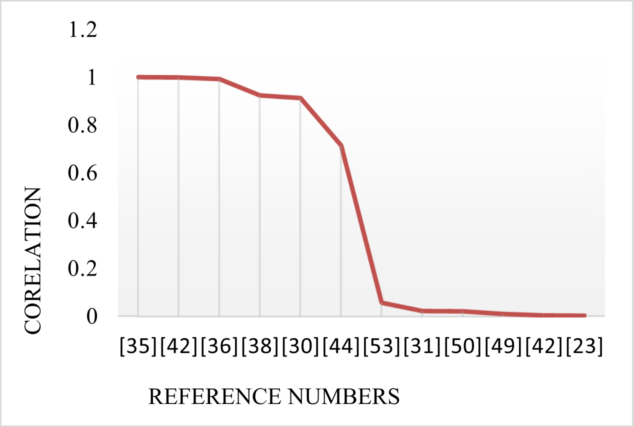


FIGURE 7. Correlational coefficient analysis.

3) INFORMATION ENTROPY ANALYSIS

Information Entropy Analysis (IEA) evaluates the degree of disorder or randomness of information in an image [23]. When the value of information entropy is high then there would be the least possibility of information leakage [64]. Here, i represents the value of pixel and $p(i)$ shows the probability of i. The entropy of a given image can be calculated as

$$\text{IEA} = -\sum_{i} p(i)\log_2 p(i) \tag{6}$$

The value of IEA should be 8 ideally for a 256 (2^8) gray level encrypted image [38]. The IEA values shown in Table 4 are the average values calculated for different images. The ideal IEA value shows that all the pixels are distributed randomly. However, it is generally less than 8 because in the original image pixels are correlated.

Table 4 shows the CCA, HA, and IEA parameters which are analyzed by the given references to show the effectiveness of the existing VMEI methods. It can be observed that most of the techniques have not evaluated all the parameters that are necessary to stop the statistical attacks.

B. PARAMETERS EVALUATING THE ENCRYPTION KEY

The encryption key used for image encryption is an important aspect of measuring the security level of the encryption technique. There are two key analysis parameters such as key space and key sensitivity.

1) KEY SPACE ANALYSIS

The key space represents the size of the key used by the image encryption method. The size of the key must be large to protest brute force attacks. It is an exhaustive task to try all the possible combinations, for example, if the n-bit key is taken,

TABLE 5. Evaluation parameters comparison for the quality of encryption key.

Reference Number	Key Space	Key Sensitivity
[5]	$37*2^{240}$	✓
[18]	10^{42}	✗
[23]	2^{418}	✓
[30]	$37*10^{68}$	✗
[31]	10^{76}	✓
[35]	10^{56}	✓
[37]	37^2*229^6	✓
[38]	10^{75}	✓
[39]	$0.49*10^{45}$	✓
[40]	10^{75}	✓
[41]	10^{56}	✓
[42]	37^2*10^{70}	✗
[43]	10^{70}	✓
[44]	10^{80}	✓
[49]	10^{105}	✗
[50]	10^{75}	✓
[54]	10^{70}	✓

then 2n combinations are possible. For an effective image encryption algorithm, key space must be at least 2100 or larger than this [31]. To persist brute force attack it should be large enough. Table 5 shows key space taken by given VMEI techniques. The computing precision is considered 10-14 in [37], [42], and [54].

2) KEY SENSITIVITY ANALYSIS

Key sensitivity ensures that a small modification in the key may create completely different results. An algorithm has good key sensitivity if an original image cannot be recovered even if there is a slight change in the key [31]. Table 5 shows the VMEI techniques, which performed a key sensitivity test of the key used for encryption.

C. EVALUATION PARAMETERS FOR THE QUALITY OF IMAGE

The encrypted image when decrypted is ideally expected to be of the same quality with no degradation as compared to the original image. VMEI technique generates an encrypted image that is visually meaningful. Therefore, the quality of the encrypted image is also taken into consideration, because when an image is implanted into a reference image, the reference image has been degraded. The Following parameters are evaluators of degradation in the quality of the image.

1) PEAK SIGNAL-TO-NOISE RATIO (PSNR) AND STRUCTURAL SIMILARITY INDEX (SSIM)

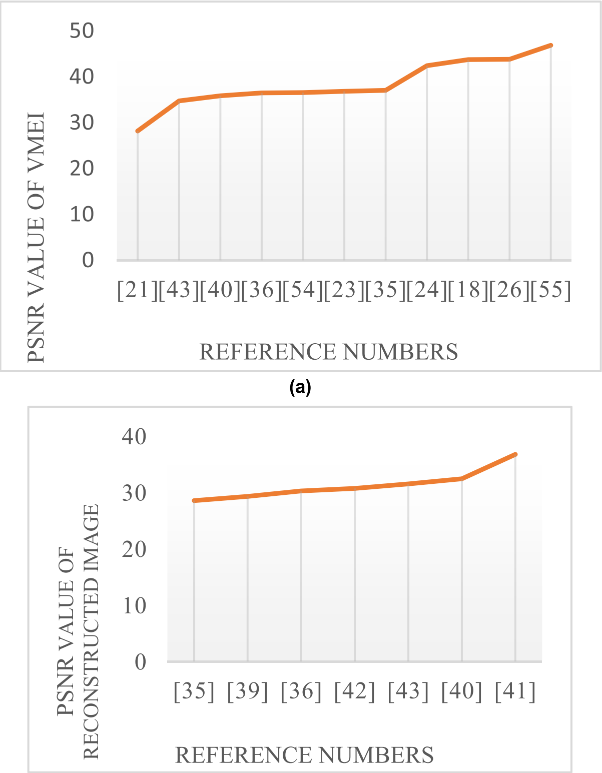
As the image is processed and transmitted over the network, then the quality of the image is degraded. PSNR and SSIM are the image visual quality evaluation parameters. That provides the difference between original and reconstructed images. It measures the pixel difference between the given two images [7]. It is calculated as

$$\mathrm{PSNR} = 10\log_{10}\frac{m^2}{\mathrm{MSE}} \tag{7}$$

Here, m represents the maximum value of the pixel. For example, if the pixel value is represented in 8 bits, then maximum value is 255. MSE stands for mean square error, which is calculated as

$$\mathrm{MSE} = \frac{\sum_{R,C}\left[I_1(r,c) - I_2(r,c)\right]^2}{R * C} \tag{8}$$

Here, R and C represent the rows and columns of the image matrix. I_1 and I_2 represent the input images, which are being compared.



(a)

(b)

FIGURE 8. PSNR value of VMEI Techniques: a) PSNR value of VMEI; b) PSNR value of reconstructed image.

The values of PSNR for a VMEI and reconstructed image should be at least 30 decibels or higher for an 8-bit image and at least 60 decibels for the 16-bit image. The higher PSNR value represents better the visual quality. Table 6 and Figure 8 shows the VMEI techniques those evaluated the PSNR of VMEI [18], [21], [23], [24], [26], [35], [36], [38], [40], [42], [54] and reconstructed image after decryption [35], [36], [37], [38], [39], [40], [41], [42]. It could be observed that Ref. [55] has higher PSNR value of VMEI as compared to other techniques which indicates that generated VMEI is almost like a reference image. Reference [41] has a higher PSNR value which shows that the quality of the reconstructed image is better than other techniques.

SSIM is used to assess luminance, contrast, and structure comparisons between original and reconstructed images [65], [66]. It is calculated among the same size windows of an

TABLE 6. Evaluation parameters comparison for the quality of VMEI and recovered images.

Reference Number	PSNR (dB)		SSIM	
	VMEI	Reconstructed	VMEI	Reconstructed
[5]	×	×	×	×
[18]	43.7831	-	0.9992	-
[21]	28.1827	-	0.8619	-
[23]	36.8660	-	×	×
[24]	42.4258	-	0.9715	-
[26]	43.8274	-	0.8584	×
[35]	37.0175	28.55	0.9874	0.9932
[36]	36.4869	30.2643	-	0.8139
[39]	-	29.2742	-	0.7308
[40]	35.8625	32.4235	0.8885	-
[41]	-	36.7526	×	×
[42]	-	30.7225	-	0.97215
[43]	34.7746	31.4930	×	×
[49]	×	×	×	×
[54]	36.5767	-	×	×
[55]	46.8684	-	×	×

TABLE 7. Parameters based on resistance of techniques against various attacks.

Reference Number	Data Loss Attack	Noise Attack	KPA and CPA
[5]	✓	GN, S&P, SN	×
[18]	✓	×	×
[23]	✓	×	×
[24]	×	GN, S&P, SN, PN, LPF, MF, Sharpen, JPEG compression	×
[35]	✓	S&P	✓
[36]	×	GN, S&P	✓
[37]	×	×	✓
[40]	✓	GN, S&P, SN	×
[41]	×	GN, S&P	×
[42]	✓	GN, S&P, SN	✓
[49]	✓	GN, SN	×

image. If x and y are two windows, then it is calculated as

$$\mathrm{SSIM} = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{9}$$

where $c_1$and c_2 are the variables to stabilize the division with weak denominator,

$$c_1 = (0.01, \mathrm{dr})^2 \, andc_2 = (0.03, \mathrm{dr})^2 \tag{10}$$

Here, dr represents the dynamic range of values of the pixel. μ_x and μ_y denote the average of an original and reconstructed image, respectively. σ_x^2 and σ_y^2 denotes the variance of x and y, respectively. σ_{xy} represents the covariance of x and y. The value of SSIM should in between -1 and 1, where 1 is an ideal value that specifies complete structural similarity and zero specifies no structural similarity. Table 6 shows the VMEI techniques that evaluated the SSIM of VMEI [18], [21], [24], [26], [35], [38], [40] and reconstructed image after decryption [35], [36], [38], [39], [42].

D. PARAMETERS BASED ON RESISTANCE OF TECHNIQUES AGAINST VARIOUS ATTACKS

1) NOISE ATTACK

An attacker may introduce different types of noise attacks to the encrypted image so that contained information could be destroyed. Therefore, an original image would not be successfully recovered after decryption. Hence, the encrypted image should be unaffected by noise attacks [40]. There are various types of noise attacks, such as Gaussian Noise (GN), Salt and Pepper noise (S&P), Speckle Noise (SN), Poisson Noise (PN), and Low Pas Filtering (LPF). Median Filter (MF), sharpen and JPEG compression, etc. Table 7 represents the VMEI techniques those performed noise attacks to show the resistance against it.

2) DATA LOSS ATTACK

When an encrypted image is transmitted over the network then because of some network fault or other faults, some data may be lost. Hence, the quality of recovered image after decryption may be affected [42]. The algorithm should be capable of handling data loss and the quality of recovered image must be unaffected. Table 7 represents the VMEI techniques that performed data loss attack to show the technique's resistance against it.

Table 7 shows that most of the existing VMEI techniques do not satisfy all the parameters. Therefore, the development of an improved VMEI technique is still an open area.

3) KNOWN PLAINTEXT ATTACKS (KPA) AND CHOSEN PLAINTEXT ATTACKS (CPA)

KPA and CPA are the types of cryptographic attacks. In KPA, the attacker knows the original image and its corresponding encrypted image. However, in CPA, the encryption method is known to the attacker, hence attacker can encrypt any randomly chosen image and get the encrypted form of that image [67]. These attacks are generally applied to find the original image by cryptanalysis. An encryption method should be effective to handle such types of attacks. Table 7 represents the VMEI techniques that perform these attacks to check the resistance of techniques against KPA and CPA.

Table 8 summarizes most of the VMEI techniques. It is observed that the issues like image security, computational speed, visual quality of reconstructed image, VMEI size, VMEI quality, etc. are addressed in the literature.

IV. APPLICATIONS OF VMEI

This section provides a survey on applications of VMEI techniques. It comprises various applications to different extents,

TABLE 8. Summarizes VMEI techniques.

Ref. No.	Advantages	Disadvantages
[18]	• Security of the method is improved by the use of chaotic maps.	• Not suitable to handle large media. • VMEI size is double as compared to original image
[23,25, 27]	• Improved security • Improved quality of VMEI	• Computational complexity • Visual quality of reconstructed image may be improved
[26]	• Improved security • Improved quality of VMEI	• Execution time • VMEI size is double as compared to original image • Visual quality of reconstructed image
[35-39]	• Improved security • Reduced size of VMEI	• Execution time • Visual quality of reconstructed image
[41]	• Improved security	• Computational complexity • VMEI size is double as compared to original image • Visual quality of reconstructed image
[42]	• Improved security • Implemented with both color and grey scale reference images.	• Time-consuming operations • VMEI size is double as compared to original image • Visual quality of reconstructed image
[44]	• Improved security	• VMEI size is double as compared to original image • Visual quality of reconstructed image • Visual quality of VMEI
[50]	• Improved security • Speed	• VMEI size is double as compared to original image • Visual quality of reconstructed image • Visual quality of VMEI

where data is stored or transferred over the computer network. Some of the applications are as follows

1) Medical Applications: When a digital medical image is exchanged among physicians over the network, the confidentiality of the image is an important factor to consider because the image may contain sensitive data [11], [68].

2) Military Applications: The secret digital images are widely used and transmitted over networks in military applications such as missile guidance, target detection and tracking, etc. [69].

3) Multimedia Applications: The important multimedia data is stored and transmitted over the network. Image encryption is widely used for secure storage and communication [70].

(4) Cloud Computing: In current technology, cloud computing is popular for providing huge data storage that can be accessed remotely. Hence, the security of images and other data are the main concern because it is stored on the network [71].

5) Internet Communication: The internet provided worldwide connected networks in which information (i.e., digital images, text audio, video, etc.) is shared over the network. It requires protection against unauthorized access, hacking, & various types of attacks [72].

6) Disaster Management: There are various uses of digital images involved in real-time monitoring of natural disasters like earthquakes, fire, floods, etc., to reach the disaster-struck areas. The authorities need to protect these images from authorized access [73].

7) Telemedicine System: In modern technology, these systems are used for medical consultation remotely. The digital images are shared between doctors and patients like prescriptions, medical reports, etc., therefore it requires encryption techniques to secure the images [55], [74].

8) Remote Sensing: The process of monitoring and capturing information remotely, typically by satellites or aircraft is called remote sensing. These images need to be protected to maintain the privacy of data [75].

9) Intelligent Transport System: The digital images are captured through the cameras in the field of traffic and vehicle management on roads to provide better services to the users. It is necessary to secure these images to avoid misuse [76].

V. FUTURE RESEARCH CHALLENGES

In this section, future research challenges are identified based on the systematic literature survey performed. It is observed from the collected work that the evolution of a potent VMEI technique is still an open area for investigation. The existing VMEI techniques suffer from various issues like poor computational speed, visual quality of reconstructed images etc. The potential future research directions based upon raised issues are:

A. COMPUTATIONAL SPEED

VMEI techniques perform encryption in two phases of encryption and embedding, so the computational burden is high. Hence, there is the requirement for a computationally fast technique that could perform rapidly by using some speed increasing technique like parallel processing.

B. VISUAL QUALITY OF RECONSTRUCTED IMAGE

In VMEI techniques, an encrypted image is implanted into the cover image. Hence, the visual quality of the recovered image is reduced. This necessitates betterment in the image quality of the recovered image.

C. ARTIFICIAL INTELLIGENCE (AI) TECHNIQUES

In the modern world, AI is one of the evolving technologies. Implementation of AI techniques like a neural network, genetic algorithm, and fuzzy logic, etc., in image processing, requires wider investigation. It could be implemented in both the phases of encryption and embedding to generate a VMEI.

D. QUANTUM COMPUTING

The abilities of quantum computing are to store an enormous amount of data, very high speed, and require less power as compared to conventional computers. The computation speed would be increased exponentially if the VMEI technique would be implemented on a quantum computer. However, the implementation of quantum computing could be complex and requires in-depth investigation.

E. BLOCK COMPRESSIVE SENSING

There are various existing VMEI techniques that have used compressive sensing to reduce the size of VMEI. It can be replaced with block compressive sensing [77], which is more efficient, simpler, requires less memory, faster reconstruction, and a lightweight compressive sensing approach.

F. IMPLEMENTATION WITH COLOR IMAGES

Most of the existing VMEI techniques are implemented on grayscale original images. So, the same techniques can be implemented with color images and performance comparison could be evaluated.

G. META-HEURISTIC BASED IMPLEMENTATION

The existing VMEI techniques use constant parameters to perform encryption as well as embedding. The improper parameter estimation may lead to poor performance. Therefore, meta-heuristic algorithms [78] can utilize to optimize the parameters to enhance the performance of VMEI techniques.

VI. CONCLUSION

This paper provided a systematic literature survey on VMEI techniques. The paper classified VMEI techniques into various categories suggested in the literature. Further, the existing VMEI techniques were compared based on various security, key analysis, visual quality, and miscellaneous parameters. It is observed that computational speed and visual quality of reconstructed images are still open areas of research. The future research scope and challenges of VMEI techniques were discussed. It has been concluded that VMEI is still an underdeveloped field. The outcomes of this state-of-the-art survey would be useful for the enhancement of digital image encryption.

REFERENCES

[1] N. K. Pareek, V. Patidar, and K. K. Sud, "Substitution-diffusion based image cipher," *Int. J. Netw. Secur. Appl.*, vol. 3, no. 2, pp. 149–160, Mar. 2011.

[2] R. C. Gonzalez and R. E. Woods, *Digital Image Processing Using MATLAB*, 2nd ed. New York, NY, USA: McGraw-Hills, 2010.

[3] V. Vučković, "Image and its matrix, matrix and its image," *Surv. Nat. Center Digitization*, no. 12, pp. 17–31, 2008. [Online]. Available: http://eudml.org/doc/254223

[4] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[5] L. Bao and Y. Zhou, "Image encryption: Generating visually meaningful encrypted images," *Inf. Sci.*, vol. 324, pp. 197–207, Dec. 2015.

[6] H. Kaur, D. Koundal, and V. Kadyan, "Image fusion techniques: A survey," *Arch. Comput. Methods Eng.*, vol. 28, no. 7, pp. 4425–4447, Dec. 2021, doi: 10.1007/s11831-021-09540-7.

[7] S. Singh, N. Mittal, and H. Singh, "Review of various image fusion algorithms and image fusion performance metric," *Arch. Comput. Methods Eng.*, vol. 28, no. 5, pp. 3645–3659, Aug. 2021, doi: 10.1007/s11831-020-09518-x.

[8] N. Kaur, I. Sbsstc, and S. Behal, "A survey on various types of steganography and analysis of hiding techniques," *Int. J. Eng. Trends Technol.*, vol. 11, no. 8, pp. 388–392, May 2014.

[9] G. Kaur, S. Singh, R. Rani, and R. Kumar, "A comprehensive study of reversible data hiding (RDH) schemes based on pixel value ordering (PVO)," *Arch. Comput. Methods Eng.*, vol. 28, no. 5, pp. 3517–3568, Aug. 2021, doi: 10.1007/s11831-020-09512-3.

[10] M. Kaur and G. Kaur, "Review of various steganalysis techniques," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 1744–1747, 2014.

[11] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[12] C. Pak and L. L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 138, pp. 129–137, Sep. 2017.

[13] H. Andrews and C. Patterson, "Singular value decomposition (SVD) image coding," *IEEE Trans. Commun.*, vol. TC-24, no. 4, pp. 425–432, Apr. 1976.

[14] M. M. Kaur and V. Kumar, "Comprehensive survey on image encryption techniques," *Arch. Comput. Methods Eng.*, vol. 27, pp. 15–43, Nov. 2018.

[15] D. Mistry and A. Banerjee, "Discrete wavelet transform using MATLAB," *Int. J. Comput. Eng. Technol.*, vol. 4, pp. 252–259, Apr. 2013.

[16] S. Thakral and P. Manhas, "Image processing by using different types of discrete wavelet transform," in *Proc. Int. Conf. Adv. Informat. Comput. Res.* Singapore: Springer, Dec. 2018, pp. 499–507.

[17] J. Cherian and A. T. Mereena, "A survey on DWT and LWT based digital image watermarking," *Int. J. Res. Comput. Appl. Inf. Technol.*, vol. 4, pp. 27–32, May 2016.

[18] A. Kanso and M. Ghebleh, "An algorithm for encryption of secret images into meaningful images," *Opt. Lasers Eng.*, vol. 90, pp. 196–208, Mar. 2017.

[19] R. Brown and L. O. Chua, "Clarifying chaos: Examples and counterexamples," *Int. J. Bifurcation Chaos*, vol. 6, no. 2, pp. 219–249, Feb. 1996.

[20] H. Lee, "Wavelet analysis for image processing," Inst. Commun. Eng., Nat. Taiwan Univ., Taipei, Taiwan, Tech. Rep., 2017. [Online]. Available: http://disp.ee.ntu.edu.tw/henry/wavelet_analysis.pdf

[21] V. M. Manikandan and V. Masilamani, "An efficient visually meaningful image encryption using Arnold transform," in *Proc. IEEE Students' Technol. Symp. (TechSym)*, Kharagpur, India, Sep. 2016, pp. 266–271.

[22] M. Boora and M. Gambhir, "Arnold transform based steganography," *Int. J. Soft Comput. Eng.*, vol. 3, pp. 136–140, Sep. 2013.

[23] Y.-G. Yang, Y.-C. Zhang, X.-B. Chen, Y.-H. Zhou, and W.-M. Shi, "Eliminating the texture features in visually meaningful cipher images," *Inf. Sci.*, vol. 429, pp. 102–119, Mar. 2018.

[24] Y. G. Yang, L. Zou, Y. H. Zhou, and W. M. Shi, "Visually meaningful encryption for color images by using Qi hyper-chaotic system and singular value decomposition in YCbCr color space," *Optik*, vol. 213, Feb. 2020, Art. no. 164422.

[25] M. Li, H. Fan, H. Ren, D. Lu, D. Xiao, and Y. Li, "Meaningful image encryption based on reversible data hiding in compressive sensing domain," *Secur. Commun. Netw.*, vol. 2018, pp. 1–12, Feb. 2018.

[26] T. Tuncer, S. Dogan, R. Tadeusiewicz, and P. Pławiak, "Improved reference image encryption methods based on 2^K correction in the integer wavelet domain," *Int. J. Appl. Math. Comput. Sci.*, vol. 29, no. 4, pp. 817–829, Dec. 2019.

[27] J. O. Armijo-Correa, J. S. Murguía, M. Mejía-Carlos, V. E. Arce-Guevara, and J. A. Aboytes-González, "An improved visually meaningful encrypted image scheme," *Opt. Laser Technol.*, vol. 127, Jul. 2020, Art. no. 106165.

[28] Y. Dong, X. Huang, and G. Ye, "Visually meaningful image encryption scheme based on DWT and Schur decomposition," *Secur. Commun. Netw.*, vol. 2021, pp. 1–16, Feb. 2021.

[29] Y.-G. Yang, B.-P. Wang, Y.-L. Yang, Y.-H. Zhou, W.-M. Shi, and X. Liao, "Visually meaningful image encryption based on universal embedding model," *Inf. Sci.*, vol. 562, pp. 304–324, Jul. 2021.

[30] W. Wen, Y. Zhang, Y. Fang, and Z. Fang, "Image salient regions encryption for generating visually meaningful ciphertext image," *Neural Comput. Appl.*, vol. 29, no. 3, pp. 653–663, Jul. 2016.

[31] X. Sun, D. Liu, Y. Ji, S. Yan, C. Li, and B. Du, "A new image block encryption method based on chaotic map and DNA encoding," in *Proc. 7th Int. Conf. Digit. Home (ICDH)*, Guilin, China, Nov. 2018, pp. 37–41.

[32] A. Hazra, S. Ghosh, and S. Jash, "A survey on DNA based cryptographic techniques," *Int. J. Netw. Secur.*, vol. 20, pp. 1093–1104, Nov. 2018.

[33] Y. Arjoune, N. Kaabouch, H. El Ghazi, and A. Tamtaoui, "A performance comparison of measurement matrices in compressive sensing," *Int. J. Commun. Syst.*, vol. 31, no. 10, p. e3576, Apr. 2018.

[34] W. Xingyuan, Z. Junjian, and C. Guanghui, "An image encryption algorithm based on ZigZag transform and LL compound chaotic system," *Opt. Laser Technol.*, vol. 119, Nov. 2019, Art. no. 105581.

[35] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105837.

[36] R. Ponuma, R. Amutha, S. Aparna, and G. Gopal, "Visually meaningful image encryption using data hiding and chaotic compressive sensing," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 25707–25729, May 2019.

[37] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Process.*, vol. 134, pp. 35–51, May 2017.

[38] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Process.*, vol. 155, pp. 218–232, Feb. 2019.

[39] F. Jie, P. Ping, G. Zeyu, and M. Yingchi, "A meaningful visually secure image encryption scheme," in *Proc. IEEE 5th Int. Conf. Big Data Comput. Service Appl.*, New York, CA, USA, Apr. 2019, pp. 199–204.

[40] P. Ping, J. Fu, Y. Mao, F. Xu, and J. Gao, "Meaningful encryption: Generating visually meaningful encrypted images by compressive sensing and reversible color transformation," *IEEE Access*, vol. 7, pp. 170168–170184, 2019.

[41] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion," *Signal Process.*, vol. 172, Jul. 2020, Art. no. 107563, doi: 10.1016/j.sigpro.2020.107563.

[42] X. Chai, H. Wu, Z. Gan, Y. Zhang, and Y. Chen, "Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107525, doi: 10.1016/j.sigpro.2020.107525.

[43] C. Pan, G. Ye, X. Huang, and J. Zhou, "Novel meaningful image encryption based on block compressive sensing," *Secur. Commun. Netw.*, vol. 2019, pp. 1–12, Nov. 2019.

[44] W. Wen, Y. Hong, Y. Fang, M. Li, and M. Li, "A visually secure image encryption scheme based on semi-tensor product compressed sensing," *Signal Process.*, vol. 173, Aug. 2020, Art. no. 107580.

[45] G. Ye, C. Pan, Y. Dong, K. Jiao, and X. Huang, "A novel multi-image visually meaningful encryption algorithm based on compressive sensing and Schur decomposition," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 2, p. e407, Feb. 2021, doi: 10.1002/ett.4071.

[46] D. Jiang, L. Liu, L. Zhu, X. Wang, X. Rong, and H. Chai, "Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform," *Signal Process.*, vol. 188, Nov. 2021, Art. no. 108220.

[47] Z. Hua, K. Zhang, Y. Li, and Y. Zhou, "Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing," *Signal Process.*, vol. 183, Jun. 2021, Art. no. 107998.

[48] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, "An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing," *Inf. Sci.*, vol. 556, pp. 305–340, May 2021.

[49] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. A. Sheikh, "Visual meaningful encryption scheme using intertwining logistic map," in *Intelligent Computing* (Advances in Intelligent Systems and Computing), vol. 857. Cham, Switzerland: Springer, Nov. 2018, pp. 779–788.

[50] J. S. Khan, J. Ahmad, S. S. Ahmed, H. A. Siddiqa, S. F. Abbasi, and S. K. Kayhan, "DNA key based visual chaotic image encryption," *J. Intell. Fuzzy Syst.*, vol. 37, pp. 2549–2561, Sep. 2019.

[51] M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in *Proc. Annu. Conf. New Trends Inf. Commun. Technol. Appl. (NTICT)*, Baghdad, Iraq, Mar. 2017, pp. 86–90.

[52] L. D. Singh and K. M. Singh, "Visually meaningful multi-image encryption scheme," *Arabian J. Sci. Eng.*, vol. 43, no. 12, pp. 7397–7407, Feb. 2018.

[53] H. R. Vanamala and D. Nandur, "Genetic algorithm and chaotic maps based visually meaningful image encryption," in *Proc. IEEE Region Conf. (TENCON)*, Kochi, India, Oct. 2019, pp. 892–896.

[54] C. Pan, X. Huang, G. Ye, and Z. Wang, "An image visual cryptography using double encryption and hiding technology," in *Proc. 3rd Int. Conf. Adv. Image Process.*, Chengdu, China, Nov. 2019, pp. 50–54.

[55] Y. Dai, H. Wang, Z. Zhou, and Z. Jin, "Research on medical image encryption in telemedicine systems," *Technol. Health Care*, vol. 24, no. 2, pp. 435–442, Jun. 2016.

[56] Y.-G. Yang, B.-P. Wang, S.-K. Pei, Y.-H. Zhou, W.-M. Shi, and X. Liao, "Using M-ary decomposition and virtual bits for visually meaningful image encryption," *Inf. Sci.*, vol. 580, pp. 174–201, Nov. 2021.

[57] X. Huang, Y. Dong, G. Ye, W.-S. Yap, and B.-M. Goi, "Visually meaningful image encryption algorithm based on digital signature," *Digit. Commun. Netw.*, May 2022, doi: 10.1016/j.dcan.2022.04.028.

[58] M. G. Abdelfattah, S. F. Hegazy, N. F. F. Areed, and S. S. A. Obayya, "Optical cryptosystem for visually meaningful encrypted images based on gyrator transform and Hénon map," *Opt. Quantum Electron.*, vol. 54, no. 2, pp. 1–22, Feb. 2022.

[59] X. Huang, Y. Dong, H. Zhu, and G. Ye, "Visually asymmetric image encryption algorithm based on SHA-3 and compressive sensing by embedding encrypted image," *Alexandria Eng. J.*, vol. 61, no. 10, pp. 7637–7647, 2022.

[60] K. Wang, M. Liu, Z. Zhang, and T. Gao, "Optimized visually meaningful image embedding strategy based on compressive sensing and 2D DWT-SVD," *Multimedia Tools Appl.*, pp. 1–25, Mar. 2022.

[61] Y.-G. Yang, B.-P. Wang, Y.-L. Yang, Y.-H. Zhou, W.-M. Shi, and X. Liao, "A visually meaningful image encryption algorithm based on adaptive 2D compressive sensing and chaotic system," *Multimedia Tools Appl.*, pp. 1–30, Jun. 2022.

[62] L. Abraham and N. Daniel, "Secure image encryption algorithms: A survey," *Int. J. Sci. Technol. Res.*, vol. 2, no. 4, pp. 186–189, Apr. 2013.

[63] V. M. S. Garcia, M. D. G. Ramirez, R. F. Carapia, E. Vega-Alvarado, and E. R. Escobar, "A novel method for image encryption based on chaos and transcendental numbers," *IEEE Access*, vol. 7, pp. 163729–163739, 2019.

[64] O. Omoruyi, C. Okereke, K. Okokpujie, E. Noma-Osaghae, O. Okoyeigbo, and S. John, "Evaluation of the quality of an image encryption scheme," *Telecommun. Comput. Electron. Control*, vol. 17, pp. 2968–2974, Dec. 2019.

[65] Y. A. Al-Najjar and D. C. Soong, "Comparison of image quality assessment: PSNR, HVS, SSIM, UIQI," *Int. J. Sci. Eng. Res.*, vol. 3, no. 8, pp. 1–5, Aug. 2012.

[66] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.

[67] N. Ahmed, H. Asif, and G. Saleem, "A benchmark for performance evaluation and security assessment of image encryption schemes," *Int. J. Comput. Netw. Inf. Secur.*, pp. 9–16, Oct. 2009.

[68] M. Sokouti, A. Zakerolhosseini, and B. Sokouti, "Medical image encryption: An application for improved padding based GGH encryption algorithm," *Open Med. Informat. J.*, vol. 10, no. 1, pp. 11–22, Oct. 2016, doi: 10.2174/1874431101610010011.

[69] E. Du, R. Ives, A. van Nevel, and J.-H. She, "Advanced image processing for defense and security applications," *EURASIP J. Adv. Signal Process.*, vol. 2010, no. 1, Dec. 2011, doi: 10.1155/2010/432972.

[70] P. P. Dang and P. M. Chau, "Image encryption for secure internet multimedia applications," *IEEE Trans. Consum. Electron.*, vol. 46, no. 3, pp. 395–403, Aug. 2000.

[71] J. Mahalakshmi and K. Kuppusamy, "An efficient image encryption method based on improved cipher block chaining in cloud computing as a security service," *Austral. J. Basic Appl. Sci.*, vol. 10, no. 2, pp. 297–306, 2016.

[72] S. P. Indrakanti and P. S. Avadhani, "Permutation based image encryption technique," *Int. J. Comput. Appl.*, vol. 28, no. 8, pp. 45–47, Aug. 2011.

[73] A. S. Maihulla, I. Yusuf, and S. I. Bala, "Reliability and performance analysis of a series-parallel system using Gumbel–Hougaard family copula," *J. Comput. Cogn. Eng.*, vol. 1, pp. 74–82, May 2022.

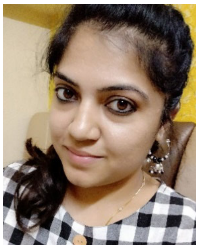
[74] S. Rajagopalan, B. Dhamodaran, A. Ramji, C. Francis, S. Venkatraman, and R. Amirtharajan, "Confusion and diffusion on FPGA—Onchip solution for medical image security," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Coimbatore, India, Jan. 2017, pp. 1–6.

[75] G. Muhiuddin, A. Mahboob, and M. E. Elnair, "A new study based on fuzzy bi-Γ-ideals in ordered-Γ-semigroups," *J. Comput. Cogn. Eng.*, vol. 1, pp. 42–46, Feb. 2022.

[76] K. T. Atanassov, "New topological operator over intuitionistic fuzzy sets," *J. Comput. Cognit. Eng.*, vol. 1, no. 3, pp. 94–102, 2022.

[77] L. Gan, "Block compressed sensing of natural images," in *Proc. Int. Conf. Digit. Signal Process.*, Jul. 2007, pp. 403–406.

[78] M. Kaur, S. Singh, M. Kaur, A. Singh, and D. Singh, "A systematic review of metaheuristic-based image encryption techniques," *Arch. Comput. Methods Eng.*, pp. 1–15, Oct. 2021, doi: 10.1007/s11831-021-09656-w.



VARSHA HIMTHANI received the bachelor's degree in information technology from Rajeev Gandhi Prodyogiki Vishwavidyalaya, Bhopal, Madhya Pradesh, India, and the master's degree in computer science from Rajasthan Technical University, Rajasthan, India. She is currently pursuing the Ph.D. degree in computer engineering with Manipal University Jaipur, Rajasthan. Since 2008, she has been an academician in the same field. Her research interests include information security and artificial intelligence.

VIJAYPAL SINGH DHAKA received the Ph.D. degree in computer science from Bhimrao Ambedkar University, Agra, India, in 2010. He is a seasoned academician with a flair for entrepreneurial spirit. He enjoys a persistent passion for continuous learning for self and students' growth. He has more than 16 years of experience in the software industry, academics, research, teaching, and training. He has more than 80 publications in journals of great repute in his name and guided ten research scholars to earn Ph.D. He has published more than six patents and acquired more than 15 copyrights on software applications and inventions. He received the "World Eminence Awards 2017" for Leading Research Contribution in ICT in 2016, at WS-4 in London in February 2017.

MANJIT KAUR (Senior Member, IEEE) received the M.E. degree in information technology from Punjab University, Chandigarh, India, in 2011, and the Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2019. She was an Assistant Professor at Chandigarh University, Mohali, India; Manipal University Jaipur, Jaipur, India; and Bennett University, Greater Noida, India. In 2021, she joined the School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju, South Korea, where she is currently affiliated. Her research interests include wireless sensor networks, digital image processing, and metaheuristic techniques. She was in the top 2% list issues by "World Ranking of Top 2% Scientists" in 2021. She was part of the 11 Web of Science/Scopus indexed conferences.

DILBAG SINGH (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the Thapar Institute of Engineering and Technology, Patiala, India, in 2019. He was an Assistant Professor at Chandigarh University, Mohali, India; Manipal University Jaipur, Jaipur, India; and Bennett University, Greater Noida, India. In 2021, he joined to the School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju, South Korea, where he is currently affiliated. He has published more than 70 research articles in SCI/SCIE indexed journals. He has also submitted five patents and has published three books and two book chapters. His H-index is 31. His research interests include image processing, computer vision, deep learning, metaheuristic techniques, and information security. He was in the top 2% list issues by "World Ranking of Top 2% Scientists" in 2021. He was part of the 11 Web of Science/Scopus indexed conferences. He was the Lead Guest Editor/an Editorial Board Member of many SCI/SCIE indexed journals, such as *Journal of Healthcare Engineering*, *Mathematical Problems in Engineering*, and *Journal of Intelligent and Fuzzy Systems*.

HEUNG-NO LEE (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the University of California, Los Angeles, CA, USA, in 1993, 1994, and 1999, respectively. He was a Research Staff Member at the HRL Laboratories, LLC, Malibu, CA, USA, from 1999 to 2002. From 2002 to 2008, he was an Assistant Professor at the University of Pittsburgh, PA, USA. In 2009, he joined the School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju, South Korea, where he is currently affiliated. His research interests include information theory, signal processing theory, blockchain, communications/networking theory, and their application to wireless communications and networking, compressive sensing, future internet, and brain–computer interface. He has received several prestigious national awards, including the Top 100 National Research and Development Award in 2012, the Top 50 Achievements of Fundamental Research Award in 2013, and the Science/Engineer of the Month, in January 2014.