Comparative Assessment of Existing Meaningful Image Encryption Techniques

V Himthani¹, V S Dhaka² and M Kaur³

¹²Department of Computer and Communication Engineering, Manipal University Jaipur, India
³Computer Science Engineering, School of Engineering and Applied Sciences, Bennett University, Noida, India

Email-varsha.himthani@gmail.com

Abstract: In recent trends, digital images are commonly used for communication, storage, medical imaging, etc. These images may contain confidential data. Image encryption and steganography are popular techniques to provide information security. In image encryption, a secret image is encoded using an encryption key, and in image steganography, a secret image is embedded in some cover media. Encrypted images are visually recognizable as these are noise-like, but stego images are visually unrecognizable. In this concern, some visually secure encryption techniques are developed, known as Meaningful Image Encryption (MIE). It includes the advantages of both image encryption and steganography. This paper provides a thorough review of existing MIE techniques. A comparative assessment based on various performance parameters is presented. Further, this paper provides the main application areas of MIE techniques. Moreover, the future research perspective to enhance the existing MIE techniques are discussed in detail.

1. Introduction

Nowadays, digital data is stored and transmitted over the internet widely. Hence, these digital data require security from the attackers. Encryption and steganography are two ways to protect confidential data. In encryption, data is encoded using a cipher key and transformed into a meaningless form [1-5]. Hence, an attacker can recognize that some secret information is hidden into it. However, in steganography, data is hidden in some cover media [6-10]. Hence, an attacker cannot easily recognize that secret information is concealed. The data can be in any form like image, text, audio, and video, etc. Digital images are encrypted by encoding or shuffling the pixels of an image using various encryption techniques [11]. When pixels are shuffled or encoded, it is transformed into a noise-like cipher image. This is a visual sign of the presence of confidential data. An attacker can easily recognize it. In image steganography, a secret image is embedded in the cover media (i.e., image, audio or video, etc.) [7]. Hence, an attacker cannot easily recognize that a secret image is hidden into cover media. To provide enhanced security and protection, Meaningful image encryption (MIE) techniques are developed.
1.1 Meaningful Image Encryption

When an image is encrypted, it is transformed into a texture-like or noise-like image, as shown in Fig. 1. These texture and noise-like images catch the attacker’s attention. Hence, an encrypted image is embedded into the cover image. So, the finally encrypted image looks like a cover image [12]. It includes the advantage of image steganography with aided security of encryption and eliminates the snag of image encryption.

![Encrypted images](image-1.png)

**Fig. 1** Encrypted images

There are two steps in MIE techniques: first, a secret image is encrypted using any existing image encryption technique that produces an encrypted noise-like image [1]. Second, an encrypted noise-like image is embedded into a cover image using the image steganography technique [6]. The outcome of the second step is a final cipher stego image (CSI) which is visually meaningful. The block diagram of MIE is shown in Fig. 2.

![Block diagram of MIE](image-2.png)

**Fig. 2** Block diagram of MIE

In this paper, a systematic literature review is performed on the existing MIE techniques. The security parameters, visual quality measures, and encryption key parameters of MIE techniques are analyzed. Further, future research challenges and opportunities for efficient MIE techniques are presented. Hence, this work would be helpful to understand and enhance the MIE techniques pertaining to the image security.

The rest of the paper is organized as: Section 2 gives the literature review of MIE techniques. Section 3 presents the analysis of MIE techniques based on various parameters. Section 4 and Section 5 give the applications and future research directions, respectively. The conclusion is presented in Section 6.
2. MIE Techniques
In recent years, various MIE techniques are proposed to provide high security to the secret image. In [12], a MIE technique is proposed to protect the secret image and transform it into a visually meaningful encrypted image in two steps. The first step is pre-encryption, which is encrypting a secret image using any existing image encryption technique. The second step is embedding the encrypted image in the cover image using Discrete Wavelet Transform (DWT). Many improvements are suggested like improved visual quality of final CSI, high covertness and improved security of technique etc. in [13-23]. Table 1 shows the literature review of various MIE techniques. It provides the encryption and embedding techniques implemented in different MIE techniques, and proposed improvements. From Table 1 it can be observed that chaotic map based encryption and DWT based embedding are used in most of the MIE techniques [17,19,21-23]. In some MIE techniques, DNA based key generation is combined with chaotic maps to enhance the security [19,22].

Encryption techniques based on chaotic maps provide high security as random keys are generated by these algorithms. Also, these techniques are fast and easy to implement. DWT is a transform domain technique in which digital image is decomposed into four sub-bands. The secret image is embedded in medium high frequencies and image will be restored by performing the inverse transformation. DWT provides good perception quality that is essential requirement of embedding. DWT is used in the second step of MIE techniques that embed encrypted secret image into cover image to generate a final CSI.

Table 1: MIE Techniques

| Reference Number | Year | Encryption Technique Used | Embedding Technique Used | Improvement Proposed |
|------------------|------|---------------------------|-------------------------|----------------------|
| [13]             | 2016 | Encryption using key      | Arnold transform and    | Visual quality of    |
|                  |      |                           | DWT                     | final CSI            |
| [14]             | 2017 | 3D chaotic Map            | 2D LWT                  | Security and visual |
|                  |      |                           |                         | quality of final CSI|
| [15]             | 2017 | Pixel shuffling and       | Hash-LSB steganography  | Security             |
|                  |      | RC4 stream cipher         |                         |                      |
| [16]             | 2017 | Key generation using      | DWT                     | Visual quality of    |
|                  |      | discrete quantum walks    |                         | final CSI            |
| [18]             | 2018 | Intertwining Logistic Map | Lifting wavelet         | Security             |
|                  |      | and Gray S BOX            | transform               |                      |
| [19]             | 2018 | Logistic chaotic map and  | DWT                     | Security             |
|                  |      | DNA coding                |                         |                      |
| [20]             | 2018 | ANY encryption technique  | Reversible Data hiding  | High covertness      |
|                  |      |                           | in compressive domain   |                      |
| [21]             | 2019 | ANY encryption technique  | Bit division, 2^n       | Visual quality of    |
|                  |      |                           | correction, Integer 2D | final CSI            |
|                  |      |                           | DWT                     |                      |
| [22]             | 2019 | DNA based key generation,| DWT                     | Noise resistance      |
|                  |      | chaotic map               |                         |                      |
| [23]             | 2019 | Logistic chaotic map,     | DWT                     | Security             |
|                  |      | Arnold Transformation and |                         |                      |
|                  |      | Genetic algorithm         |                         |                      |
| [17]             | 2020 | Qi hyper-Chaotic          | DWT, DCT                | Security and visual  |
|                  |      |                           |                         | quality of final CSI|


After encryption and embedding stage through MIE techniques, the size of the final CSI increases as compared to the secret image [24]. The compressive sensing-based image encryption techniques are used to decrease the size of the final CSI. These techniques implemented image compression with simultaneous encryption and used a measurement matrix as the secret key. In the second phase, a compressed, encrypted image is embedded in the cover image. Table 2 shows the MIE techniques based on compressive sensing. In these MIE techniques, the size of the final CSI is decreased as compared to original secret image. However, the visual quality of reconstructed secret image suffers due to compression.

**Table 2: Compressive Sensing based MIE techniques**

| Reference Number | Year | Encryption method | Embedding Method |
|------------------|------|-------------------|------------------|
| [26]             | 2016 | DWT then zig-zag confusion, compressive sensing, SHA-256 hash function, Skew tent chaotic map | DWT |
| [27]             | 2018 | Parallel compressive sensing and zigzag confusion, Logistic tent chaotic map | 3D cat map, Integer discrete wavelet transform |
| [24]             | 2019 | Zig-zag confusion and compressive sensing | dynamic LSB |
| [25]             | 2019 | DWT then zig-zag confusion and chaotic map based compressive sensing | DWT |
| [28]             | 2019 | DWT, zig-zag confusion and compressive sensing 2D logistic-adjusted-sine chaotic map | Integer wavelet transform |
| [29]             | 2019 | DWT, compressive sensing 2D logistic-adjusted-sine chaotic map | Images are divided into blocks and fitted |
| [32]             | 2019 | DWT, zig-zag confusion, logistic-Tent map, compressive sensing | DWT, 2 level-DCT |
| [30]             | 2020 | DWT, zig-zag confusion, logistic-Tent map, compressive sensing. | DWT, Singular Value Decomposition |
| [31]             | 2020 | DWT, Singular Value Decomposition, Logistic chaotic system, 4D hyper-chaotic system, SHA 256, Local binary pattern | Integer Wavelet Transform |
| [33]             | 2020 | DWT, Tent chaotic map, Arnold Transform | 2D DWT |

3. Performance comparison based on evaluation parameters
The proposed MIE techniques aim to construct high security. The security level of methods is evaluated by different parameters [34-40]. Based on protection provided by various MIE techniques, a comparison is presented on the basis of key space analysis (KSA), correlation coefficient (CC), and information entropy (IE).

The KSA denotes the critical size used in image encryption. It should be large enough to protect against brute force attacks. The CC analysis (CCA) evaluates the correlation between two pixels of an image. It should be nearly zero. The correlation zero indicates no correlation between the pixel and its neighbor pixel. For an embodiment, if \( p \) denotes a pixel value and \( q \) is its neighbor pixel value, \( STD \) is standard deviation, then the correlation coefficient can be calculated as:
IE analysis evaluates the degree of uncertainty in the image information. If \( p(x) \) is the probability of occurrence of pixel value \( x \), then IE for an encrypted image can be calculated as

\[
IE = - \sum_x p(x) \log_2 p(x)
\]  

(2)

The high IE value (ideally maximum 8 for image size 256×256) indicates the most negligible probability of information leakage because of random pixel distribution [37]. The IE values presented in Table 3 represent the average value calculated for different images.

The reconstructed image is expected to be the same in visual quality as the original secret image. MIE techniques generate visually meaningful cipher images. An encrypted image is embedded in the reference image. Therefore, the visual quality of the final cipher image is also taken into consideration. This is because embedding an image in an image degrades the visual quality of the reference image.

Peak signal to noise ratio (PSNR) is the evaluation of change in pixel of a reconstructed image compared to the original secret image. PSNR evaluation is based on the pixel difference between the original reference and embedded reference images [40]. If \( x \) denotes the maximum pixel value and \( E \) represents the mean square error, then it can be calculated as:

\[
PSNR = 10 \log_{10} \frac{x^2}{E}
\]  

(3)

For an 8-bit image, the PSNR value should be at least 30 decibels or higher. The high PSNR signifies the better visual quality of embedded reference images than the original reference image [41]. The low image quality indicates the presence of a hidden image, hence attract the attacker’s attention.

Table 3 shows the performance comparison of MIE techniques. It can be observed that KSA and IE values are satisfactory in most of the MIE techniques. However, there is not a single method for that all the parameters evaluation brings good results.
4. Applications of MIE

MIE comprises several applications in different areas, where digital images are communicated or stored over the internet. It can be implemented in the field of the medical and health sector for secure communication of medical images among doctors through the internet [42]. Nowadays, remote medical consultation is also widespread; a patient can online consult and share health reports with the doctor [43]. Similarly, it can be implemented in military or defense communications to maintain the confidentiality of data [44]. The MIE can also be used in many other applications like cloud storage [45,46,47], remote sensing [46], satellite [49,50], etc.

5. Future Research Challenges

It is observed from the detailed literature survey performed on various existing MIE techniques that the advancement of these techniques is still an open area for research. The current MIE techniques undergo some unavoidable issues. In existing MIE techniques, an image is encrypted and then embedded in a reference image. Hence, the visual quality of the reconstructed secret image is degraded and needs to be amended. To improve the visual quality of the final cipher and reconstructed images, deep learning algorithms can be applied to embed an encrypted image in the reference image.

Moreover, deep learning algorithms would also reduce the size of the final meaningful cipher image. Many researchers have implemented compressive sensing-based algorithms to reduce the size of the final cipher image, but it degrades the image quality. Further, it is observed that the existing MIE techniques could achieve high security if quantum cryptography is used for encryption [51].

6. Conclusion

In this paper, basic concept of various existing MIE techniques and compressive sensing-based MIE techniques are presented in detail. The performance of different MIE techniques is analysed based on various evaluation parameters. Further, the future research scopes to potentially enhance the existing methods are discussed. It could be observed from this study that visual quality of the final CSI and reconstructed image requires improvement from an image security perspective. The size of final CSI must be reduced without using compression as it decreases the image quality. The conclusions of this study would be helpful for the enrichment of image security.

References

[1] Kaur M and Kumar V 2018 Comprehensive survey on image encryption Techniques Archives of Computational Methods in Engineering 27 pp 15–43

[2] Kumari M, Gupta S and Sardana P 2017 A survey of image encryption algorithms 3D Res 8 37 Springer https://doi.org/10.1007/s13319-017-0148-5

[3] Kathi P, Goyal S and Agrawal R 2017 Survey on various image encryption schemes through chaotic maps International Journal of Advanced Research in Computer Science Udaipur 8

[4] Sankpal P and Vijaya P 2014 Image encryption using chaotic maps: A Survey 2014 Fifth International Conference on Signal and Image Processing pp 102-107 10.1109/ICSIP.2014.80

[5] Murugan C A and Kumar P K 2018 Survey on image encryption schemes, Bio-cryptography and Efficient Encryption Algorithms Mobile Networks and Applications https://doi.org/10.1007/s11036-018-1058-3

[6] Kadhim I J, Premaratne P, Vial P J and Halloram B 2018 Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research Neurocomputing https://doi.org/10.1016/j.neucom.2018.06.075
[7] Akhtar N, Khan S and Johri P 2014 An improved inverted LSB image steganography. International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) pp 749-755 doi:10.1109/ICICT.2014.6781374.

[8] Singh A and Singh H 2015 An improved LSB based image steganography technique for RGB images. 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) pp 1-4 doi:10.1109/ICECCT.

[9] Cheddad A, Condell J, Curran K and Kevitt P M 2010 Digital image steganography: Survey and analysis of current methods. Signal Processing 90 pp 727-752.

[10] Subramanian N, Elharrouss O, Somaya A M and Bouridane A 2021 Image steganography: A review of the recent advances. IEEE Access 9 10.1109/ACCESS.2021.3053998.

[11] Pareek N K, Patidar V and Sud K K 2011 Substitution-diffusion based image cipher. International Journal of Network Security & Its Applications 3 pp 149-160.

[12] Bao L and Zhou Y 2015 Image encryption: Generating visually meaningful encrypted images. Information Sciences 324 pp 197-207.

[13] Yang Y G et al 2018 Eliminating the texture features in visually meaningful cipher images. Information Sciences 429 pp 102-119.

[14] Manikandan V M and Masilamani V 2016 An efficient visually meaningful image encryption using Arnold transform. 2016 IEEE Students’ Technology Symposium (TechSym) Kharagpur.

[15] Abood M H 2017 An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT) Baghdad.

[16] Kanso A and Ghebleh M 2017 An algorithm for encryption of secret images into meaningful images. Optics and Lasers in Engineering 90 pp 196-208.

[17] Yang Y et al 2020 Visually meaningful encryption for color images by using Qi hyper-Chaotic system and singular value decomposition in YCrCb color space. Optik.

[18] Abbasi S F et al 2018 Visual meaningful encryption scheme using intertwining logistic map. Advances in Intelligent Systems and Computing 857 pp 764-773.

[19] Sun X et al 2018 New Image Block Encryption Method Based on Chaotic Map and DNA Encoding. 2018 7th International Conference on Digital Home (ICDH) Guilin China pp 37-41.

[20] Li M et al 2018 Meaningful Image Encryption Based on Reversible Data Hiding in Compressive Sensing Domain. Security and Communication Networks 2018 9803519.

[21] Tuncer T, Dogan S, Tadeusiewicz R and Plawiak P 2019 Improved reference image encryption methods based on 2k correction in the integer wavelet domain. International Journal of Applied Mathematics and Computer Science 29 pp 817-829.

[22] Khan J S et al 2019 DNA key based visual chaotic image encryption. Journal of Intelligent & Fuzzy Systems 37 pp 2549-2561.

[23] Vanamala H R and Nandur D 2019 Genetic Algorithm and Chaotic Maps based Visually Meaningful Image Encryption. TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON) Kochi India pp 892-896.

[24] Chai X et al 2020 An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. Optics and Lasers in Engineering 124.

[25] Ponuma R, Amutha R, Aparna S and Gopal G 2019 Visually meaningful image encryption using data hiding and chaotic compressive sensing. Multimed Tools Appl 78 pp 25707–25729.

[26] Chai X et al 2017 A visually secure image encryption scheme based on compressive sensing. Signal Processing 134 pp 35-51.
[27] Wang H et al 2019 A visually secure image encryption scheme based on parallel compressive sensing Signal Processing 155 pp 218-232
[28] Fu J et al 2019 A Meaningful Visually Secure Image Encryption Scheme 2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService) Newark CA USA pp 199-204
[29] Ping P et al 2019 Meaningful Encryption; Generating Visually Meaningful Encrypted Images by Compressive Sensing and Reversible Color Transformation in IEEE Access 7 pp 170168-170184
[30] Ye G et al 2020 Image encryption and hiding algorithm based on compressive sensing and random numbers insertion Signal Processing 4 107563 10.1016/j.sigpro.2020.10756
[31] Chai X et al 2020 Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy Signal Processing 171 https://doi.org/10.1016/j.sigpro.2020.107525
[32] Pan C, Ye G, Huang X and Zhou J 2019 Novel meaningful image encryption based on block compressive sensing Security and Communication Networks 2019 6572105
[33] Wen W et al 2020 A visually secure encryption scheme based on semi-tensor product compressed sensing Signal Processing 173 107580
[34] Omoruyi O et al 2019 Evaluation of the quality of an image encryption scheme Telecommunication Computing Electronics and Control 17 pp 2968-2974
[35] Wang Z et al 2004 Image quality assessment: from error visibility to structural similarity IEEE Transaction on Image Processing 13 pp 600–612
[36] Mali K, Chakraborty S and Roy M 2015 A Study on Statistical Analysis and Security Evaluation Parameters in Image Encryption International Journal for Scientific Research & Development 3
[37] Asuero A G, Sayago A and González A G 2006 The correlation coefficient: An overview Critical Reviews in Analytical Chemistry 36 pp 41–59 10.1080/10408340500526766.
[38] Núñez J A, Cincotta P M and Wachlin F C 2006 Information Entropy In: Muzzio J.C., Ferraz-Mello S., Henrard J. (eds) Chaos in Gravitational N-Body Systems. Springer https://doi.org/10.1007/978-94-009-0307-4_4
[39] Ahmed N, Asif HMS and Saleem G 2009 A Benchmark for performance evaluation and security assessment of image encryption schemes International Journal of Computer network and Information Security pp 9-16
[40] Hore A and Ziou D 2010 Image quality metrics: PSNR vs. SSIM ' in Proceedings of IEEE International. Conference on Pattern Recognition. pp 2366-2369
[41] Kumar A 2018 A Review on Implementation of Digital Image Watermarking Techniques Using LSB and DWT’ In Third International Conference on Information and Communication Technology for Sustainable Development
[42] Dai Y et al 2016 Research on medical image encryption in telemedicine systems Technology and Health Care 24 pp S435-S442
[43] Rajagopalan S et al 2017 Confusion and Diffusion on FPGA – Onchip solution for medical image security International Conference on Computer Communication and Informatics (ICCCI - 2017) Coimbatore INDIA
[44] Du E et al 2011 Advanced Image Processing for Defense and Security Applications EURASIP Journal on Advances in Signal Processing 2010 432972 https://doi.org/10.1155/2010/432972
[45] Rad P, Muppidi M, Jaimea A S, Agaian S S and Jamshidi M 2015 A novel image encryption method to reduce decryption execution time in cloud Annual IEEE Systems Conference (SysCon) Proceedings pp 478-482 10.1109/SYSCON.2015.7116797
[46] Kakkad V, Patel M and Shah M 2019 Biometric authentication and image encryption for image security in cloud framework Multiscale and Multidisciplinary Modeling, Experiments and Design 2 pp 233–248
[47] Kumar A 2019 Design of Secure Image Fusion Technique Using Cloud for Privacy-Preserving and Copyright Protection International Journal of Cloud Applications and Computing (IJCAC) pp 22-36
[48] Yin L, Zhao J and Duan Y 2008 Encryption Scheme for Remote Sensing Images Based on EZW and Chaos The 9th International Conference for Young Computer Scientists Hunan pp 1601-1605
[49] Murtaza A and Jianwei L 2018 A simple, secure and efficient authentication protocol for real-time earth observation through satellite 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST) Islamabad pp 822-830
[50] Bentoutou Y, Bensikaddour E H, Taleb N and Bounoua N 2020 An improved image encryption algorithm for satellite applications Advances in Space Research 66 pp 176-192
[51] Yan F et al 2017 Quantum image processing: A review of advances in its security technologies International Journal of Quantum Information 15 1730001