Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, July, 2021: 5108 - 5123

A Systematic Review on Spatial Domain Steganography & Cryptography Techniques

D.Arul Suresh[1,] Dr.R.Balasubramanian[2]
[1]Research Scholar, [2]Professor
Department of Computer Science and Engineering,
Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli
***Corresponding Author: suresharul93@gmail.com**

ABSTRACT

The establishment of secure communication between two communicating parties is becoming a difficult problem due to the possibility of attacks and other unintentional changes during active communication over an unsecured network. Secret information, on the other hand, can be safeguarded using either cryptography or steganography. Steganography is the practise of concealing a message (with no traceability) in such a way that it has no meaning to anyone other than the intended recipient, whereas cryptography is the art of converting a plaintext (message) into an unreadable format. Thus, steganography hides the existence of a secret message, whereas cryptography modifies the message format itself. Steganography and cryptographic techniques are both powerful and resilient. The primary goal of this paper is to examine various methods for combining steganography and cryptographic techniques to create a hybrid system. Furthermore, some distinctions between cryptographic and steganography techniques were presented.

Keywords: Information hiding, Cryptography, Image steganography, Security, Image quality

1 INTRODUCTION

Every day, a massive amount of data is produced as a result of recent technological advancements in digitization. Storing, transmitting, and sharing this sensitive information over an open and insecure communication channel remains a challenge [1]. Researchers have shown a great deal of interest in data security techniques such as cryptography, watermarking, and steganography. Figure 1 depicts how different data security techniques are classified. Indeed, these three security techniques are so similar that their primary goal is to maintain data confidentiality during transmission. However, the guiding paradigms and working principles differ.

As a result, Table 1 compares these two security techniques to provide a clear understanding of their functionalities and to eliminate ambiguity. Various cutting-edge reviews on steganography and steganalysis have been published in the literature. The following sections highlight the proposed study's major contributions.

1. Various cutting edge research articles ranging from infant to matured ISTs have been reviewed.
2. Further, the complete list of available IS parameters are discussed at length. Next, utilizing these parameters, a comparative analysis of the referred techniques is presented.
3. Also, the major issues and underlying benefits that exist with various spatial domain ISTs are presented with an accomplished illustration of each.

4. Additionally, the recent developments in this field, particularly with the advent of machine learning (ML) based ISTs are also discussed.
5. Finally, some promising future directions to look forward in this domain have been suggested.

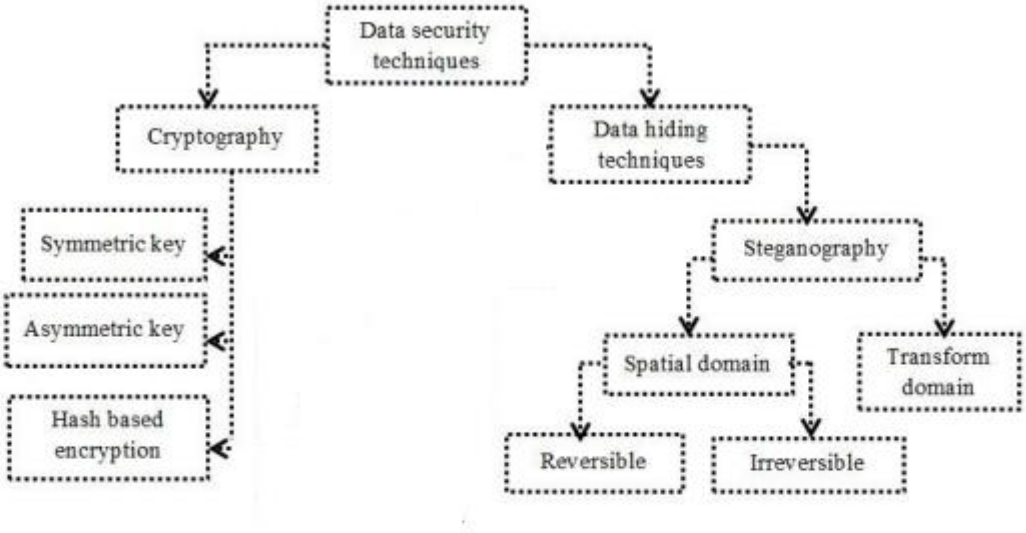
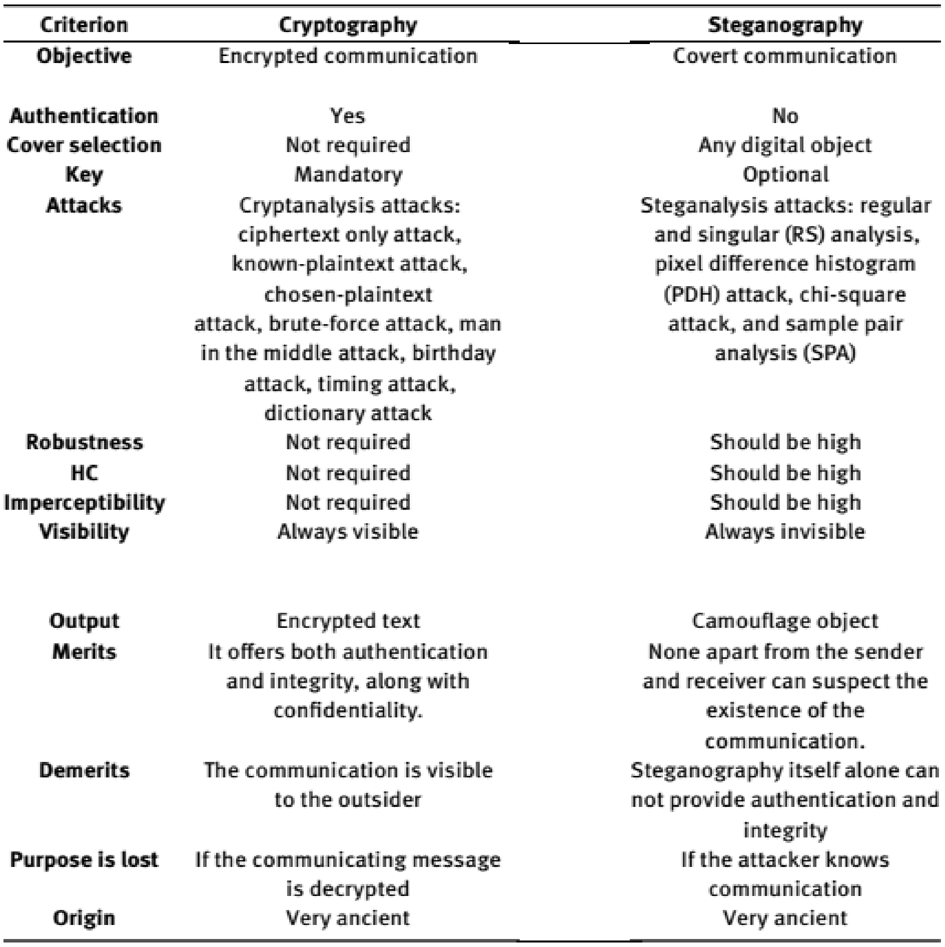


Fig 1: Classification of data security techniques

Table 1: Comparison of the working principles for cryptography and Steganography



Criterion	Cryptography	Steganography
Objective	Encrypted communication	Covert communication
Authentication	Yes	No
Cover selection	Not required	Any digital object
Key	Mandatory	Optional
Attacks	Cryptanalysis attacks: ciphertext only attack, known-plaintext attack, chosen-plaintext attack, brute-force attack, man in the middle attack, birthday attack, timing attack, dictionary attack	Steganalysis attacks: regular and singular (RS) analysis, pixel difference histogram (PDH) attack, chi-square attack, and sample pair analysis (SPA)
Robustness	Not required	Should be high
HC	Not required	Should be high
Imperceptibility	Not required	Should be high
Visibility	Always visible	Always invisible
Output	Encrypted text	Camouflage object
Merits	It offers both authentication and integrity, along with confidentiality.	None apart from the sender and receiver can suspect the existence of the communication.
Demerits	The communication is visible to the outsider	Steganography itself alone can not provide authentication and integrity
Purpose is lost	If the communicating message is decrypted	If the attacker knows communication
Origin	Very ancient	Very ancient

2 DATA SECURITY TECHNIQUES

Around 4000 years ago, ancient Egyptians used logographic scripts or characters known as 'hieroglyphs' for secret communication. Later, these pictographic forms became the foundation of cryptography, giving rise to various digital cypher techniques such as mono-alphabetic substitution and Caesar shift. Cryptography is the art of secret writing that involves converting secret information into a meaningless or unintelligible form. This can be accomplished by employing mathematical theories and computational intelligence. Figure 2 depicts the general working principle of cryptographic communication between sender and receiver. The fundamental components of cryptographic systems are

(1) The information which has to be securely transmitted (plaintext)

(2) The encryption algorithm, which uses secret information to transform the plaintext into an absurd form (cipher text)

(3) The decryption algorithm for retrieving the secret information

(4) The key generally the encryption and decryption algorithms require the use of keys for encryption and decryption.

As a result, in order to make the encryption computationally unbreakable, the keys must be strong and kept in a secure location. As a result, the keys are crucial to achieving a high level of confidentiality. The cryptographic keys are classified as either secret or public. Secret keys are those that are only known to the originator and the intended receiver. Public keys, on the other hand, are known to all. Cryptanalysis is the process of decrypting encrypted data in order to retrieve sensitive information. From hieroglyphs to World War II, cryptography has been widely used, primarily for secure communications between sender and receiver. Cryptography has recently become the foundation of a wide range of modern-day applications. Figure 3 depicts some of the applications of cryptography.

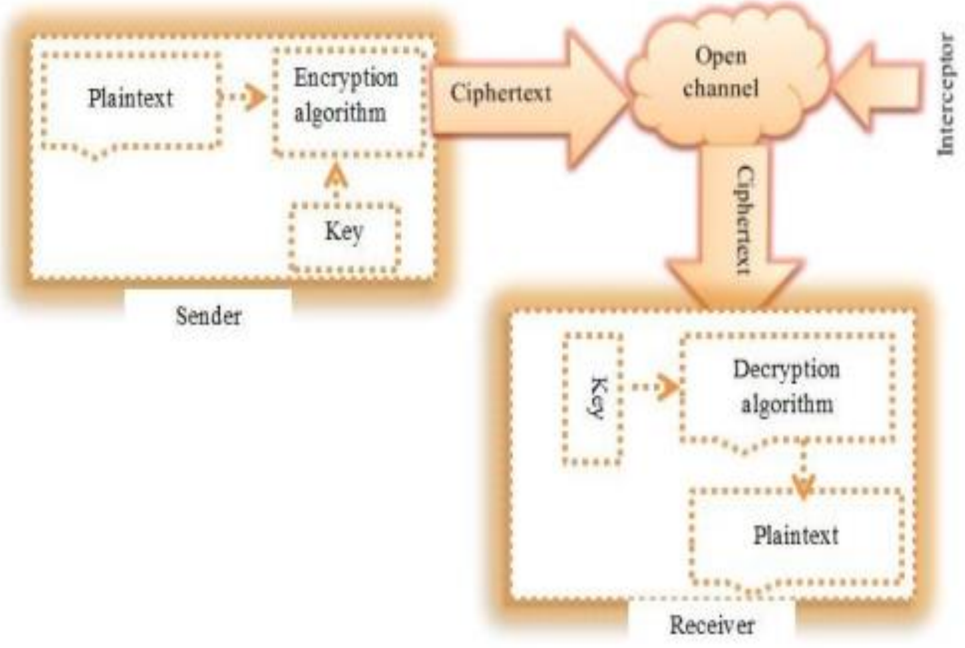


Fig. 2 – Structure of Cryptography Communication Process

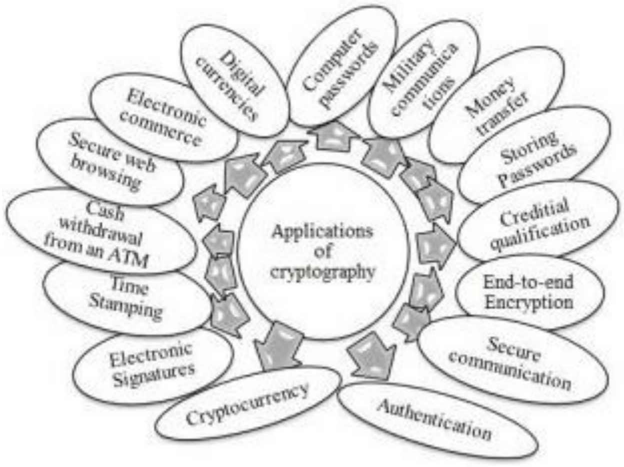


Fig.3 – Application of Cryptography

2.1 STEGANOGRAPHY

Steganography's basic concept is to conceal the existence of the secret communication from the unintended recipient. Steganography's potential has grown exponentially with advances in digitization. Because the core concept of steganography communication is transmission secrecy, it is better suited for applications where encryption-based communication is restricted. Steganography is now an integral part of a wide range of IoT-enabled industry applications, including smart cities, medical imaging, and military applications. The process of embedding and extracting steganography is depicted in Figure 4. Steganography appears to be a two-edged sword to the untrained eye. Steganography is popular among antisocial elements for covert communication due to its invisibility property. Figure 5 depicts several real-world steganography applications.

2.1.1 TYPES OF STEGANOGRAPHY

There are different types of steganography according to the carrier type described in [2], [3] these are text steganography, image steganography, audio/video steganography and protocol steganography

Text Steganography: In text steganography, the secret message hidden in the arrangement of text or in the form of a number of bits. It is more difficult to recognize the information hiding based on the text. This is achieved by using capital letters, white spaces and by bolding the letters [3], [4].

Audio/Video Steganography: Audio/Video steganography is a very secure steganography technique. In this technique, we hide our secret message in the audio/video file. It could not be recognized by the attacker, the intruder or third party. Audio steganography works with MP3, WAV and AU formats and video steganography work on MP4, MPEG, and AVI etc. [4], [5].

Protocol Steganography: To hide the confidential data in the protocol (that is used to send the data) called protocol steganography. In this technique, we hide our secret message in unused bits of considered network protocol [2], [5].

Image Steganography: In image steganography, we hide the confidential data into the image. Then send this Stego image over the internet. Image steganography technique is a more secure technique. The Least Significant Bit (LSB) mostly used the technique to embed the secret message in the cover image that is a more common and simple approach [2]–[5].

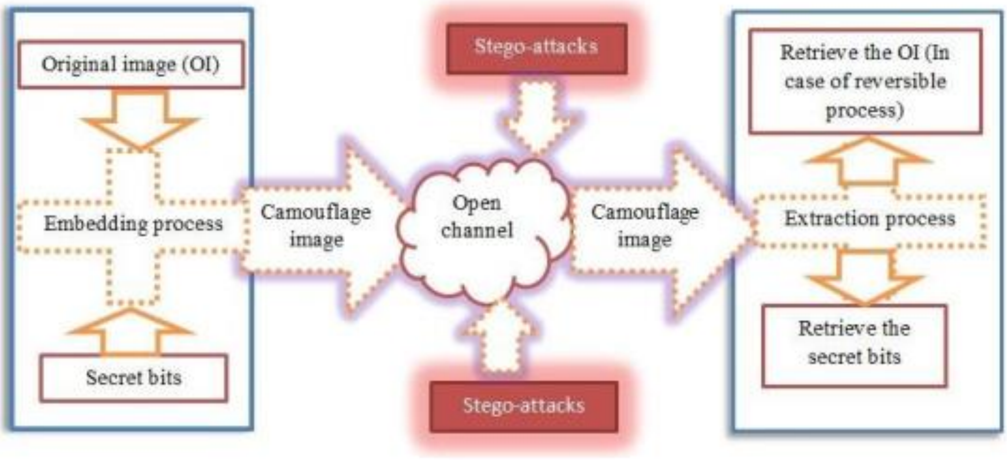


Fig.4 – Structure of Steganography Process

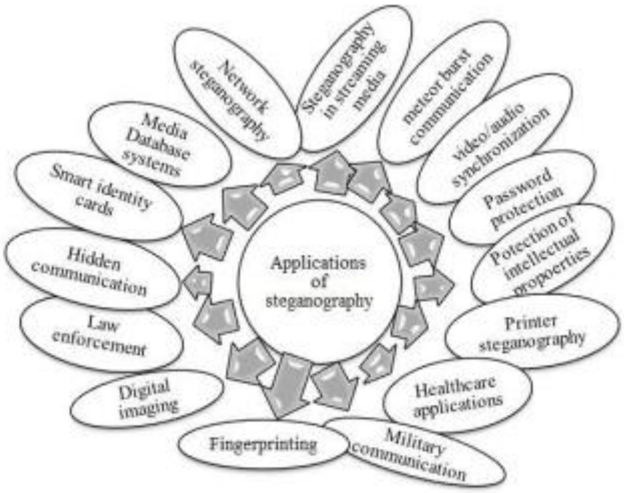


Fig.5 – Applications of Steganography

The stenographic process uses various digital objects as the carrier signals such as image, text, DNA, video, audio, and text, etc. Due to the property of innocence of digital images, researchers have preferred images as the carrier signal for hiding secret information. Also, the presence of redundant pixels in an image makes it even more suitable for embedding secret information. Hiding confidential information inside the image is known as image steganography (IS). However, most of the techniques presented in the literature were highly focused on either the spatial or transform domain. Spatial domain techniques depend solely on the pixels of the image for data embedding. Mostly, direct manipulation of the OI pixels is performed to achieve the objective. Therefore, spatial domain techniques are simple and less time-consuming. On the other hand, transform domain techniques utilize the frequency content, and they are based on orthogonal transformation (frequency and phase) to the image. In the transform domain, applying various transformations and inverse transformations, such as Fourier, Laplace, and Z the embedding process is carried out. Some common transform domain techniques are

1. Discrete Fourier transformation (DFT)
2. Discrete wavelet transformation (DWT)

3. Discrete cosine transformation (DCT)
4. Singular Value Decomposition.

The classification of spatial domain ISTs is depicted in Figure 6. The original image (OI) is the single input image used for sending secret data in the context of IS. In the same way, the camouflage image (CI) is the output image that contains the secret information. The confidential message that the sender wishes to send to the receiver is referred to as secret information. Finally, the embedding and extraction algorithms are data hiding algorithms that are used to embed and extract the secret bits.

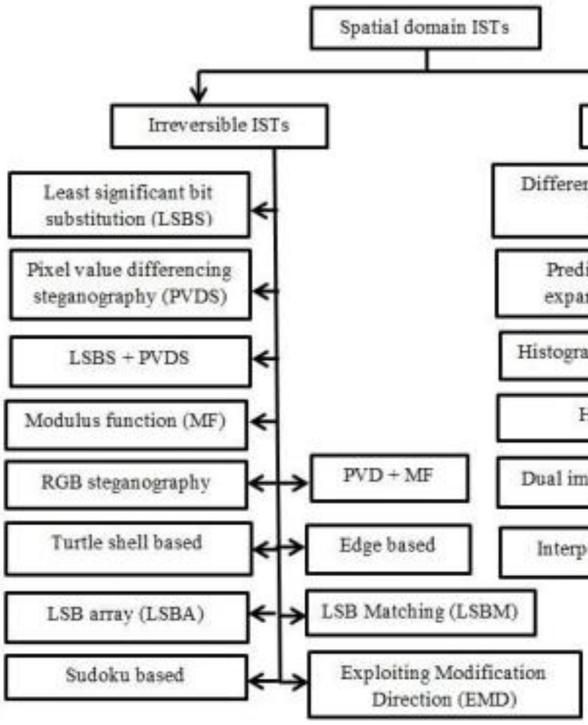


Fig.6 – Classification of Spatial Domain Steganography

3. RELATED WORKS

A literature overview of recent publications is shown in Table 2 based on cryptographic and stenographic algorithms, as well as the type of input data and cover medium taken into account to ensure secure data transmission. The results of each study are analysed using parameters such as PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error), Entropy, Histogram, Maximum embedding capacity, SSIM (Structural Similarity Index Metric), CR (Compression Ratio), and so on.

Table.2 - Overview of the Literature Survey

		Methods used	Input	Cover	

Papers	**Year**	**Cryptography**	**Steganography**	**data type**	**medium**	**Features**
“Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm”, M. Indra Sena Reddy,...[17]	2016	AES	DWT+LSB	Text	DWTImage	Higher Security, Data embedded in wavelet transformed image
“Cryptography Based Technique For Security Of Data Using Image Processing ”,Harshita Mall,...[20]	2016	AES	2DWT	Text	Image	Excellent VQ, Easy and user friendly, Good Security, capacity
“Image Steganography Method Using K-Means Clustering and Encryption Techniques”,Bhagya Pillai,..[23]	2016	DES	Kmeans, LSB	Text	Image	High Security, secure from man in the middle attack, accurate results in small time
“Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function”,Rini Indrayani,..[25]	2016	AES	Audio	Any	Audio	Excellent Audio Quality and High Capacity
“A Combined Approach of Steganography and Cryptography Technique based on Parity Checker and Huffman Encoding”,Abdelmged A.A, ,...[27]	2016	RC4	Parity check	Text	Image	Good VQ, High Capacity, Medium PSNR
“Improved diagonal queue medical image steganography using Chaos theory, LFSR, andRabin cryptosystem”,Mamta Jain, Anil Kumar,….. [29]	2016	Rabin cryptosystem	LSB	Text	Image	High PSNR, Complexity, Imperceptibility , Good Capacity, Excellent VQ
“A DCT-based Robust Video Steganographic Method Using BCH Error Correcting Codes",Ramadhan J. Mstafa,...[31]	2016	BCH codes	2D-DCT	Text	Video	Good VQ, Performance,High Capacity, Quite Robust
“Integrating RSA Cryptography & Audio Steganography”,Ankit Gambhir,...[32]	2016	RSA	LSB	Text	Audio	Good Audio Quality,High Capacity, Security

“Image and Text Steganography with Cryptography using MATLAB”,M.Saritha,...[33]	2016	Symmetric XOR	Sequential	Text	Image	High Security, user friendly
“An Enhanced Audio In Audio Hiding Model By Combining Watermarking, Steganography And Cryptography”,Arya.G.S,.. [35]	2016	Audio Cryptography	EWM, Indirect LBS-R.	Audio	Audio	High Perceptual transparency, hiding capacity and robustness
"Multiple layer Text security using Variable block size Cryptography and Image Steganography"Shivani Chauhan ,….[6]	2017	V- DES	M-LSB , RST	Text	Image	Excellent VQ, High Value of PSNR, Capacity, Low MSE,Entropy slightly high
“A Secure Data Communication System Using Enhanced Cryptography and Steganography”,Darshana Patil,..[7]	2017	EC	LSB	Text	Image	High PSNR, Capacity,Imperceptibility, Low Robustness
“An Efficient Image Cryptography using Hash- LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms”,May H.Abood [9]	2017	RC4, RGBps	HLSB	Image	Image	Efficient, high security, easy , good VQ
“Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography & Steganography”,Ria Das,.. [10]	2017	(XOR+ DES) MD5	S-LSB, V-LSB	Text	Image	Better security and privacy, Excellent VQ
“Multilayer Security Using RSA Cryptography and Dual Audio Steganography”,Kripa N Bangera ,... [14]	2017	RSA	Dual LSB	Text	Audio	High Security, Good Audio Quality
“Metamorphic cryptography considering concept of XOR and Chaotic sequence”,Namrata Singh,... [15]	2017	Chaotic sequencce	XOR+ LSB	Text	Video	Good Robustness, large payload ,Good VQ, Less distortion
“E-Banking Security using Cryptography, Steganography and Data Mining”,Namrata Devadiga,...[16]	2017	AES	F5,DBSCAN	Text	Image	High Security, High efficiency, Good VQ,prevent online frauds
“An Encryption based on DNA cryptography and	2017	DNA - AES	LSB, Adjacent	Text	DNA sequence	High Security, Capacity, low

Steganography”,Sajisha K S,... [18]						modification rate
“Secure Data Transmission techniques using AES cryptography along with Image Steganographic analysis”,ManjuBala,... [19]	2017	AES	LSB/ DCT/ DWT	Text	Image	Strong privacy, secure key transmission, better results for LSB followed by DWT then DCT.
“Enhance the Hiding Image by Using Compression and Securing Techniques ”,Ahmed S. Farhan,...[21]	2017	RC4	LSB	Image	Image	Good VQ, performance, high speed
“A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm”,B.Karthikeyan,…..[22]	2017	Double DES	LSB	Text	Image	Excellent VQ, High security during transmission
“Combining Steganography and Cryptography on Android Platform to Achieve high level security”,Sarkar Hasan Ahmed, ..[26]	2017	EPA	LSB	Text	Image	Secure and robust data transmission
“An Approach to Secure Communication using Steganography with Cryptography in an AudioFile using GA”,Amba Mishra,…..[28]	2017	Symmetric	GA,LSB	Text	Audio	High Robustness and High Security
”Enhancing Data Security Using DES-based Cryptography and DCT-based Steganography”,Achmad Solichin,... [34]	2017	DES	DCT	Text	Image	Good VQ, High Security during transmission
"Enhancing PC Data Security via Combining RSA Cryptography and Video Based Steganography”,Nouf A. Al-Juaid,...[8]	2018	RSA	3-LSB	Text	Video	Low Security, High Capacity
“Concealing Of Data Using Cryptography And Steganography”,S.S.V.S.Ramaraju ,….[11]	2018	RSA	LSBR	Text	Image	Good VQ, HighImperceptibility
“Securing Data using Elliptic Curve Cryptography and least significant bit steganography”,Jayati Bhadra,…. [12]	2018	ECC	LSB+ DCT	Text	Image	Excellent VQ, Good Embedding Capacity, security,

						Medium Imperceptibility
“Design and Development of Image Security Technique by Using Cryptography and teganography: A Combine Approach”,Aumreesh Kumar Saxena,...[13]	2018	symmetric	LSB	Image	Image	High Security, Good VQ, Low entropy and correlation ,medium PSNR
“An Improved Method for Reversible Data Hiding Steganography Combined with Cryptography”,Ms Rashmi N,..[24]	2018	AES	LSB,Improved RDH	Text	Image	Enhanced Security,Better VQ for colour than gray images ,High PSNR
“Joint Crypto-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering”,Amna Shifa,..[30]	2018	AES	LSB-M	Image	Image	High SSIM, PSNR,Efficiency, Confidentiality, Less complex, Good VQ
“Secure Data Transfer using RSA and Steganography” Khuma ZN[45]	2019	RSA	DCT	Text	Image	Hugh Security
“A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network” XINTAO DUAN et.al[36]	2020	Image Steganography	DCT	Text	Image	Improve the anti-detection property of the obtained image
“A Multi-Scale Feature Selection Method for Steganalytic Feature GFR” XINQUAN YUet.al[37]	2020	Image Steganography	GFR – Steganalytic	Text	Image	to improve the stego image detection accuracy
“Recent Advances of Image Steganography With Generative Adversarial Networks” JIA LIUet.al[38]	2020	Image Steganography	GAN Based Steganography	Text	Image	High Security, user friendly
“Comprehensive Criteria-Based Generalized Steganalysis Feature Selection Method” YIHAO WANGet.al[39]	2020	Image Steganography	CGSM	Text	Image	Good VQ, High Security during transmission
“A Novel Grayscale Image Steganography Scheme Based on Chaos Encryption and Generative Adversarial Networks” XIAOYU	2020	Image Steganography	Chaos Encryption	Text	Image	High Robustness and High Security

WANG et.al[40]						
"MUHAMMAD ZAFAR IQBAL et.al[41]	2020	IRD	LSB	Text	Image	To embed more secret information
"Steganographic Techniques Classification According to Image Format" Khaldi[43]	2020	Image Steganography	DCT	Text	Image	Precise Colormetric Representation
"A safe and secured iris template using steganography andcryptography" Abikoye[48]	2020	DES	Kmeans, LSB	Text	Image	High Security, secure from man in the middle attack, accurate results in small time period
"Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels" García-Guerrero[49]	2020	AES	LSB	Text	Image	Enhanced Security, Better VQ for colour than gray images ,High PSNR
"A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network" Duan, X et.al[50]	2020	AES	Audio	Any	Audio	Excellent Audio Quality and High Capacity
"A steganographic method based on optimized audio embedding technique for secure data communication in the internet of things" Anguraj, S et.al[51]	2020	Image Steganography	LSB	Text	Image	High Security, accurate results in small time period
"Coverless VoIP Steganography Using Hash and Hash. Cybern" Deepikaa[52]	2020	AES	Video	Text	Image	Enhanced Security,High PSNR
"Steganalysis of Quantization Index Modulation Steganography" Wu Z et.al[53]	2020	RSA	Audio	Any	Audio	Excellent Audio Quality and High Capacity
"Fast Steganalysis Method for Voip Streams" Yang H et.al[54]	2020	Image Steganography	Video	Text	Image	High Security
" AMR-WB Steganalysis based on Hybrid Classifier" Chen M et.al[55]	2020	Image Steganography	DWT	Text	Image	High Accuracy

“. Detection of heterogeneous parallel steganography for low bit-rate VoIP speech streams” Huang,Y et.al[56]	2020	Image Steganography	Audio	Any	Video	Good VQ, High Security during transmission
“Steganographic ANALYSIS of Piece message in bittorrent protocol” Xing J et.al[57]	2020	Image Cryptography	LSB	Text	Image	Secure and robust data transmission
“Secure Data Transfer over Internet Review” Dakhaz Mustafa Abdullahet.al[42]	2021	Image Steganography	LSB	Text	Image	Hugh Security Transmission
“Categorization of spatial domain techniques in image steganography: A revisit” Haref QMet.al[44]	2021	Image Steganography	DCT	Text	Image	Good VQ, High Security during transmission
“Secure Iot integration in daily lives: A review” Ameen SY[46]	2021	DES	DCT	Text	Image	Good Quality, High Security during transmission
“FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review” Yazdeen AA et.al[47]	2021	Image Steganography	FGPA	Text	Audio	High Security, user friendly
“Steganography and Steganalysis in Voice over IP: A Review” Zhijun Wu[58]	2021	Audio Cryptography	Parity check	Text	Image	Good VQ, High Capacity, Medium PSNR

4. CONCLUSION

This Review is an extensive view of various image steganography and steganalysis techniques in the spatial domain. In addition, the taxonomy of image steganography techniques and the performance evaluation metrics are also discussed. Also, the results of various image steganography techniques with respect to the three diametrically opposed steganography metrics are reported. Further, the existing issues and promising future scopes are also highlighted. Finally, in this era of digitization, steganography and steganalysis both are flourishing at a faster pace.

REFERENCES

[1] Martin.A, Sapiro.G, Seroussi.G, ”Is image steganography natural”, IEEE Transactions on Image processing,Vol.14(12),2040-2050, 2005.

[2] J. Kour, “Steganography Techniques A Review Paper”, Int. J. Emerg. Res.Manag. & Technology, vol. 9359, no. 5, pp. 132135, 2014.

[3] S. Kaur, “Steganography and Classification of Image Steganography Techniques” International Conference on Computing for Sustainable Global Development (INDIACom), pp. 870-875,2014

[4] G. Swain and S. K. Lenka, "Classification of Image Steganography Techniques in Spatial Domain: A Study", Int. J. Comput. Sci. Eng. Technol., vol. 5, no. 3, pp. 219-232, 2014.

[5] Rakhi , Suresh Gawande, "A Review On Steganography", Int. J. Adv. Res.Electr. Electron. Instrum. Eng., vol. 2, no. 10, pp. 4635-4638, 2013.

[6] Shivani Chauhan, Jyotsna, Janmejai Kumar, Amit Doegar, "Multiple layer text security using variable block size cryptography and image steganography," 3rd IEEE International Conference on Computational Intelligence and Communication Technology, pp. 1-7, 2017.

[7] Darshana Patil, Prof. P. M. Chawan, "A secure data communication system using enhanced cryptography and steganography," International Journal of Innovative Research in Computer and Communication Engineering, vol. 5, issue 6, pp. 1120-11227, June 2017.

[8] Nouf A. Al-Juaid, Adnan A. Gutub, Esam A. Khan, "Enhancing PC data security via combining RSA cryptography and video based steganography," Journal Of Information Security And Cybercrimes Research , vol. 1, no. 1, pp. 8-18, June 2018.

[9] May H. Abood, "An efficient image cryptography using Hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," Annual Conference on New Trends in Information & Communications Technology Applications, pp. 86-90, 7-9 March 2017.

[10] Ria Das, Punyasha Chatterjee, "Securing data transfer in IOT employing an integrated approach of cryptography & steganography," International Conference on High Performance Compliation, Computing and Communications, pp. 17-22, March 22-24, 2017.

[11] S.S.V.S.Ramaraju, K.Sarika, Sattibabu, A.V.S.S.Varma, "Concealing Of Data Using Cryptography And Steganography," International Journal of Research in computer and communication Technology , Vol 7, Issue 3,pp. 75-80, March 2018.

[12] Jayati Bhadra, M.K.Banga, M.Vinayaka Murthy, "Securing Data using Elliptic Curve Cryptography and least significant bit steganography," International Conference On Smart Technology for Smart Nation, pp. 1460-1466, 2017.

[13] Aumreesh Kumar Saxena, Dr.Sitesh Sinha, Dr. Piyush Shukla, "Design and development of image security technique by using cryptography and steganography: a combine approach," International Journal of Image, Graphics and Signal Processing, vol.10, no.4, pp. 13-21, April 2018.

[14] Kripa N Bangera , Yashika Paddambail , Dr.N.V. Subba Reddy, Shivaprasad G ,"Multilayer security using RSA cryptography and dual audio steganography," 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology , pp. 19-20, May 2017.

[15] Namrata Singh, Munesh Chandra Trivedi, Virendra Kumar Yadav, Vikash Kumar Singh, "Metamorphic cryptography considering concept of XOR and Chaotic sequence," 9th International Conference on Information Technology and Electrical Engineering, 2017.

[16] Namrata Devadiga, Harshad Kothari, Hardik Jain, Smita Sankhe, "E- Banking security using cryptography, steganography and data mining," International Journal of Computer Applications (0975 – 8887) , vol. 164 ,No. 9,pp. 26-30, April 2017.

[17] M. Indra Sena Reddy, Dr. A.P. Siva Kumar, "Secured data transmission using wavelet based steganography and cryptography by using AES algorithm," International Conference on Computational Modeling and Security, pp. 62 – 69, 2016.

[18] Sajisha K S, Dr. Sheena Mathew, "An Encryption based on DNA cryptography and steganography," International Conference on Electronics, Communication and Aerospace Technology, pp. 162- 167, 2017.

[19] ManjuBala, "Secure data transmission techniques using AES cryptography along with Image steganographic analysis," International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 4, Issue- 4, pp. 21-24, December 2017.

[20] Harshita Mall, M.P.S. Chawla, “Cryptography based technique for security of data using image processing,” Journal of Control and Instrumentation Engineering , vol. 2, issue. 3, pp. 5-16, 2016.

[21] Ahmed S. Farhan, Fouad H. Awad, Saif Saad, “Enhance the hiding image by using compression and securing techniques,” Iraqi Journal for Computers and Informatics (IJCI), Vol.43, Issue.1, pp 14-16, 2017.

[22] B.Karthikeyan, A. Deepak, K.S.Subalakshmi, Anishin Raj M M, V.Vaithiyanathan, “A Combined approach of steganography with LSB encoding technique and DES algorithm,” 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, 2017.

[23] Bhagya Pillai, Mundra Mounika, Pooja J Rao, Padmamala Sriram,“Image steganography method using K-Means clustering and encryption techniques,” International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1206- 1211, Sept. 2016.

[24] Ms Rashmi N, Dr Jyothi K, “An improved method for reversible data hiding steganography combined with cryptography,” 2nd International Conference on Inventive Systems and Control (ICISC 2018), pp. 81- 84, 2018.

[25] Rini Indrayani, Hanung Adi Nugroho, Risanuri Hidayat, Irfan Pratama, “Increasing the security of MP3 steganography using AES encryption and MD5 Hash function,” 2nd International Conference on Science and Technology-Computer(ICST), 2016

[26] Sarkar Hasan Ahmed, Aram Mahmood Ahmed, Omed Hasan Ahmed, “Combining steganography and cryptography on android platform to achieve high level security,” Journal Of Engineering and Applied Sciences, vol. 12, Issue 17, pp. 4448-4452, 2017.

[27] Abdelmged A. A, Al-Hussien Seddik Saad, Nada Hussien, “A Combined approach of steganography and cryptography technique based on parity checker and huffman encoding”, International Journal of Computer Applications,Vol.148, No.2, pp. 26-32, August 2016.

[28] Amba Mishra, Prashant Johri, Anuranjan Mishra, “An approach to secure communication using steganography with cryptography in an audio file using GA,” International Journal of Innovations & Advancement in Computer Science (IJIACS), Vol. 6, Issue 12, pp. 24-31, December 2017.

[29] Mamta Jain, Anil Kumar, Rishabh Charan Choudhary, “Improved diagonal queue medical image steganography using chaos theory, LFSR, and rabin cryptosystem,” Brain Informatics, pp 95-106, 2017.

[30] Amna Shifa, Muhammad S. Afgan, Mamoona N. Asghar , Martin Fleury,Imran Memon, Saima Abdullah , And Nadia Rasheed, “Joint crypto-stego scheme for enhanced image protection with nearest- centroid clustering,” vol. 6, pp. 16189-16206, April 2018.

[31] Ramadhan J. Mstafa, Khaled M. Elleithy, “A DCT-based robust video steganographic method using BCH error correcting codes,” IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016.

[32] Ankit Gambhir, Sibaram Khara “Integrating RSA cryptography & audio steganography,” International Conference on Computing, Communication and Automation (ICCCA2016), pp. 481-484, 2016.

[33] M.Saritha, Sushravya.M, Vishwanath.M. Khadabadi, “Image and text steganography with cryptography using MATLAB,” International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), pp. 584- 587, 2016.

[34] Achmad Solichin, Erwin Wahyu Ramadhan,”Enhancing data security using DES-based cryptography and DCT-based steganography,” 3rd International Conference on Science in Information Technology, pp. 618- 621, 2017.

[35] Arya.G.S, Baiju.P.S, “An enhanced audio in audio hiding model by combining watermarking, steganography and cryptography,” International Journal of Informative and Futuristic Research, vol. 3, Issue 7, March 2016.

[36] Xintao Duan , Daidou Guo , Nao Liu , Baoxia Li , Mengxiao Gou And Chuan Qin” A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network”, 10.1109/ACCESS.2020.2971528 VOLUME 8, 2020.

[37] Xinquan Yu, Yuanyuan Ma , Ruixia Jin, Lige Xu, And Xintao Duan “A Multi-Scale Feature Selection Method for Steganalytic Feature GFR”, 10.1109/ACCESS.2020.2981738VOLUME 8, 2020

[38] Jia Liu , Yan Ke , Zhuo Zhang , Yu Lei, Jun Li, Minqing Zhang, And Xiaoyuan Yang” Recent Advances of Image Steganography With Generative Adversarial Networks”, 10.1109/ACCESS.2020.2983175,VOLUME 8, 2020

[39] Yihao Wang , Yuanyuan Ma , Ruixia Jin , Pei Liu, And Ning Ruan “Comprehensive Criteria-Based Generalized Steganalysis Feature Selection Method”, 10.1109/ACCESS.2020.3018709VOLUME 8, 2020.

[40] Qi Li 1, Xingyuan Wang , Xiaoyu Wang” A Novel Grayscale Image Steganography Scheme Based on Chaos Encryption and Generative Adversarial Networks”, 10.1109/ACCESS.2020.3021103,VOLUME 8, 2020.

[41] Ghazanfar Farooq Siddiqui , Muhammad Zafar Iqbal , Khalid Saleem” A Dynamic Three-Bit Image Steganography Algorithm for Medical and e-Healthcare Systems”, 10.1109/ACCESS.2020.3028315VOLUME 8, 2020.

[42] Khaldi, "Steganographic Techniques Classification According to Image Format," International Annals of Science. Vol.8, pp.143-149,2020

[43] Haref QM, Taha MS, M. Rahim MS, Hashim MM, Ahmad AMB. Rifa'i, “Categorization of spatial domain techniques in image steganography: A revisit," Journal of Advanced Research in Dynamical and Control Systems.Vol. 10: 1538-1551, 2021.

[44] Khalid LF, Ameen SY. "Secure Iot integration in daily lives: A review," Journal of Information Technology and Informatics.Vol.1:6-12., 2021.

[45] Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Yahia HS, Mahmood MR. et al. "Comprehensive survey of big data mining approaches in cloud systems," Qubahan Academic Journal. 2021; 1:29-38.

[46] Yazdeen AA, Zeebaree SR, Sadeeq MM, Kak SF, Ahmed OM, Zebari RR. "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review," Qubahan Academic Journal. Vol.1:8-16, 2021.

[47] Shi, Y.Q.; Kim, H.-J.; Perez-Gonzalez, F. “Digital Forensics and Watermarking; Springer Science and Business Media LLC:Berlin/Heidelberg”, Germany, 2020.

[48] Abikoye, O.C.; Ojo, U.A.; Awotunde, J.B.; Ogundokun, R.O. “A safe and secured iris template using steganography andcryptography”. Multimed. Tools Appl. 2020.

[49] García-Guerrero, E.E.; Inzunza-González, E.; López-Bonilla, O.R.; Cárdenas-Valdez, J.R.; Tlelo-Cuautle, E. “Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels.Chaos Solitons Fractals Interdiscip”. J. Nonlinear Sci. Nonequilibrium Complex Phenom. 2020, 133,

[50] Duan, X.; Guo, D.; Liu, N.; Li, B.; Gou, M.; Qin, C. “A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network”. IEEE Access 2020, 8, 25777–25788.

[51] Anguraj, S.; Shantharajah, S.; Emilyn, J.J. “A steganographic method based on optimized audio embedding technique for secure data communication in the internet of things” Comput. Intell., 36, 557–573,2020.

[52] Deepikaa, S.; Saravanan, R. “Coverless VoIP Steganography Using Hash and Hash” Cybern. Inf. Technol. 20, 102–115, 2020.

[53] Wu, Z.; Li, R.; Yin, P.; Li, C. “Steganalysis of Quantization Index Modulation Steganography in G.723.1 Codec”, Future Internet, 2020.

[54] Yang, H.; Yang, Z.L.; Bao, Y.J.; Liu, S.; Huang, Y.F. Fast Steganalysis Method for Voip Streams. IEEE Signal Process. Lett., 27,286–290,2020.

[55] Wu, Y.; Chen, M.; Cao, R.; Sun, Y. AMR-WB Steganalysis based on Hybrid Classifier. Commun. Technol., 53, 2418–2424,2020

[56] Hu, Y.; Huang, Y.; Yang, Z.; Huang, Y. Detection of heterogeneous parallel steganography for low bit-rate VoIP speech streams. Neuro computing, 419, 70–79.2021.

[57] Xing, J.; Zhai, J.; Liu, W. Steganographic ANALYSIS of Piece message in bittorrent protocol. Comput. Appl. Softw. Vol.37, 315–320, 2020.

[58] Zhijun Wu, Junjun Guo , Chenlei Zhang and Changliang Li “Steganography and Steganalysis in Voice over IP: A Review” 21, 1032,2021.