Data Hiding and Watermarking Techniques: A Survey

Anoop Kumar Chaturvedi
Research Scholor
Department of Computer Science & Engineering,
University Institute of Technology, Rajiv Gandhi
Proudyogiki Vishwavidyalaya Bhopal, India

Piyush Kumar Shukla
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, Rajiv Gandhi
Proudyogiki Vishwavidyalaya, Bhopal, India

ABSTRACT
Internet is used as a leading object for simple and effective communication because of advancements technology and science. Several users access the internet and maintain their information by the help of various medium in secure and effective way. Security of information is provided by digital water marking and cryptographic techniques for patent defences, fiddle recognition and content authentication of digital information. In this paper, a widespread survey of several techniques for data hiding are explained briefly which deals with secure and private multimedia information and its accuracy. In the information hiding procedure, cryptography and steganography have assumed a noteworthy part in digital media. Information encryption keys shared by image supplier and beneficiary for image encoding and decoding. In the meantime information covering up keys additionally used to install and remove the implanted information from advanced image and obtained the cover pictures. At the extraction side if both secret key and hided information is available than unique information can be recuperated effectively. On the off chance that the beneficiary has keys for both the encryption and information hiding than it can remove the extra information and recuperate the original image.

Keywords
Watermarking, Data Hiding, Cryptography

1. INTRODUCTION
As the improvements of processing power and Internet have brought about the boundless utilization of digital information. The data sanctuary advances of computerized information have requisite for a safe communication of the sensitive information. There are two advances: cryptosystem and steganography. Steganography fluctuates from cryptography. Main focus of the cryptography approach is to make highly secured data transfer where original image are transform into other so intruder don't get real data in between. While a Steganography platform is a technique where other medium is used for transfer the secret data [1, 2]. It has a tendency to hide the nearness of the message itself, which makes it troublesome for an interloper to understand where the message is. At times, sending encoded data may draw consideration, while invisible data won't. Likewise, cryptography isn't the best answer for secure correspondence; it is just piece of the arrangement. The two sciences can be utilized together to better ensure data. For this situation, regardless of whether steganography down, the message can't be recouped in light of the fact that a cryptography method is utilized too.

The sensitive information is installed / entrenched, and image deformation happened while the image pixel position value in the original image in the information hiding system [4]. The deformation impact the issue in insightful images. Yet trivial modifications are caused by the prospective danger of the misdiagnosis for medical images [3]. These days, the reversible and irreversible information hiding examination has turned out to be significant issue. The reversible information hiding systems are inquired about to enhance the deformation in delicate images. The implanting procedure of this strategy is a portion of the common information hiding plan. Although, the elimination procedure has an extra strategy in correlation with common information hiding plan and the extra technique is the same as per the following. After the inserted sensitive information is removed, the original image can be totally reestablished to its cover position [3].

With the huge measures of sight and sound, security issues may emerge, and copyright insurance of continuously transmitted media has turned out to be one of the significant research themes. Other than encryption systems, information covering up or watermarking is another route for copyright assurance or information confirmation [4]. Execution assessments can incorporate the accompanying:

- *Reversibility*, at the decoder, cover image and sensitive data embedded in advance ought to be back in original form. Sensible measure of side data might be fundamental for extraction.
- *Embedding capacity*, which signifies the quantity of bits reasonable for embedding away into the image. Higher capacity would be more ideal.
- *Image quality* ought to be as similarity between output image and its cover counterpart.

Keeping in mind the end goal to acquire a more profound understanding of the image information hiding procedure, it is important to abbreviate the meanings of the accompanying terms and ideas:

- *Reversibility*: capacity to separate an original image from the watermark image [3].
- *Perceptibility*: perceptual comparison between the innovative and the watermarked images;
- *Payload*: watermark encoded bits excluding the repetitive data [3].
- *Robustness*: capacity to identify the stego images after the basic signal preparing tasks
- *Capacity*: installed / entrenched bits into the flag.

Figure (1) depicts the existing data hiding techniques [1].

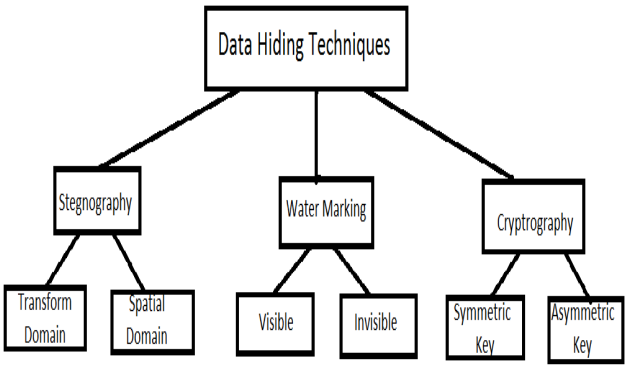

Fig 1. Data Hiding Techniques

Information hiding methods are mostly classified into 3 techniques such as Steganography, Water marking and Cryptosystem. The Steganographic process can be technical related to language whereas the watermarking process can be vigorous or brittle. Watermarking is a unique type of robust data hiding method which can further be subdivided as visible or invisible watermarking. Cryptography consist the encryption and decryption procedures which are based on symmetric and asymmetric key distribution. Figure.1 represents the whole organization of a variety of data hiding techniques [5].

1.1 Steganography

Steganography is a procedure of furtive communication [40] where a portion of information (a private message) is concealed into another portion of naive looking information, generally called a cover, in such a manner that the very subsistence of the furtive information [19] remains hidden without increasing any distrust in the minds of the audience [4].

1.1.1 Transform Domain

The information (i.e. image) is first transformed into time and frequency domain and then the message is implanted into another message in transform domain process. It is more vigorous against the modification and statistical attacks [19, 40].

1.1.2 Spatial Domain

The more admired spatial domain techniques obtain benefit of the human visual structure and directly implant information by modifying the pixel intensities [19, 40]. They are more admired because of their cleanness and simplicity of use.

1.2 Water Marking

A digital watermarking is a process to insert bits pattern into a digital information file i.e. audio, image and video [5, 7]. Such information frequently bears copyright messages of the digital file. Digital watermarking is further divided in two parts visible and invisible [12, 23].

1.2.1 Visible Watermarking

It is a visible semi-transparent image or text overload on the cover image providing copyright protection of logical property [5,7]. Visible water marking technique has a drawback of allowing the cover image to be viewed.

1.2.2 Invisible Watermarking

It is a process to embed image with messages which is not visible to the human eyes. Only copyright owner can extract the hidden messages and visible watermarks by using some specialized software [5, 7].

1.3 Cryptography

Cryptography is a process to convert the information file (i.e. image, text, audio, video etc.) into unreadable format called cipher text file by using encryption techniques [34, 39] and attributes (i.e. keys). Cryptographic is divided into two groups.

1.3.1 Symmetric Cryptography

It is a technique in which a single key is used for encryption and decryption on both ends sender and receiver. This key is generated by both sender and receiver or is transferred over internet from sender to receiver [34].

1.3.2 Asymmetric Cryptography

It is also known as public key cryptography in which a pair of keys private and public keys is used for encryption and decryption for providing confidentiality and authentication [39].

Table 1. Watermarking versus Steganography [18]

Data Hiding Technique	Contents/ Usual values	Application of the technique	Types	Properties
Steganography	• Vigour • Message confidentiality • capability • perfection – should be high for all these contents	For secret data transmission such as Military Data, Medical data etc.	Spatial domain	1. Technical cleanness & simplicity of use. 2. Capability & perfection are high. 3. Message confidentiality is very high but vigour against statistical attacks is normally low.
			Transform domain	1. Difficult to develop and employ. 2. Capability is lower than Spatial Domain. 3. Message confidentiality, perfection and vigour are high
Watermarking	• Vigour • Message confidentiality - Should be high • capability- not significant as a tiny amount of embedded data • perfection – Depends	For Copyright substantiation and verification	Visible	1. Higher order bit planes are commonly embedded. 2. Perfection is low as for the visible watermark. 3. Vigour is high
			Invisible	1. Selected pixels of the entire image are embedded. 2. Perfection is high. 3. Vigour is high. 4. High protection against illegal modification of the watermark.

Table 2. Comparison of Watermarking, Steganography and Cryptography [1]

Criterion	**Watermarking**	**Steganography**	**Cryptography**
Key	Elective	Elective	Compulsory
Visibility	Habitually	Certainly not	Forever
Type of attack	Image dispensation	Steganalysis attacks	Cryptanalysis attacks
Input files	Minimum two	Minimum two	One
Secret data	Watermark data	Payload field	Plain text file
Carrier	Nearly image	Digital media files	Mainly text files
Detection	Enlightening	Unsighted	Unsighted
Result	Watermarked data	Stego data file	Ciphertext file
Fails when	It is substituted	It is found	Deciphered
Authentication	Developed by cross correspondence	Complete recovery information	Complete recovery of information
Concern	Vigour	Capability	Vigour
Flexibility	Limitation on cover data file	Liberated to select the selection	Not given any cover

Objective	Copyright security	Private communication	Data files security
History	Recent epoch	Prehistoric	Recent epoch

2. LITERATURE REVIEW

Information hiding [1, 28] is generally performed by a lower associate or a path manager. The image proprietor can't believe the associate or path manager whole. In such situations, when the proprietor desires to maintain the sensitive of the original image, firstly he may perform encryption of the image by utilizing a cryptographic key [25]. The path director, with no information about the first image [40] content, needs to conceal information into the encrypted image utilizing an information hiding key [22, 23]. It is additionally wanted that the collector can remove the hided information and recoup the first image in a distinct [16, 29] way. Distinguishable shows, if the recipient is having the information hiding key no one but, he can remove the information, however can't decode the image [14, 23]. In the event that he has cryptographic key just, it is conceivable to decode the image, however can't extricate the hided information [19]. In the event that the collector is having both cryptographic and hiding keys, he can remove concealed information and recoup first image [32, 24]. A large portion of the work deals with information embedding and elimination on original image. Reversible information embedding away by histogram moving is depicted in [10]. In [11] information is covered up into the histogram of pixel contrasts. Information covering up in [12] stores information by manufacturing improvements to least significant bits. Various image cryptosystems have additionally been created in excess of years. Cryptographic calculations [14, 16] cataract under two common classes: substitution [24] and transposition [16]. A few calculations achieve both to improve sanctuary. Encrypted substitution rolls out improvements to the pixel position value to construct the substance mysterious. A substitution construct image cryptosystem is situated in light of pixel esteem alteration [21]. Change construct encryption calculations are situated in light of pixel rearranging. In stage based cryptosystem the pixels are rearranged and no modification is completed to the pixel position value [18]. There are various plans which perform information covering up and encryption mutually. In a little of them, a piece of cover image is utilized to convey extra information and respite of the image is encrypted case, as said in [13], watermark is embedded to abundancy of data control transmission (DCT) coefficients, and movement vector contrast, intra-expectation approach and indications of DCT coefficients are encoded. A reversible information hiding system in encrypted image is portrayed in [14], which hide information into whole encoded image. Although, in this technique image decoding and information exclusion are not detachable. The technique in [6] conceals information into a encrypted image in a distinguishable way.

Loads of research has been done in the zone of reversible information covering up. In most recent couple of years different proficient techniques have been proposed for reversible information covering up. In [6] recommends a novel technique for distinct reversible information covering up. Here substance proprietor at first scrambles the main uncompressed picture using an encryption key to make an encoded picture [3]. By then, the data hider packs the scarcest gigantic bits (LSB) of the encoded picture by means of a data concealing key to make a lacking gap to oblige the supplementary data. At the beneficiary part, the data installed in the influenced gap to can be simply recouped from the encrypted picture embedding supplementary data on the basis of data concealing key [18, 25]. While the data embeddings just impacts the LSB, a disentangling with the cryptographic key can realize a picture like the main shape. When utilizing both of the encryption and information covering up keys, the inserted extra information can be effectively removed [32, 38] and the first image can be consummately back in original formed by abusing the spatial relationship in common image [21, 25].

A reversible information hiding plan in light of histogram change displayed [7, 16]. They misuse a double tree structure to take care of the issue of conveying sets of pinnacle focuses. Dissemination of pixel contrasts is utilized to accomplish vast hiding limit while keeping the contortion low [37]. They additionally receive a histogram moving method to forestall flood and sub-current. Execution examinations with other existing plans are given to exhibit the predominance of the proposed plot [30]. The issue of transmitting repetitive information [7] over an uncertain, transfer speed compelled correspondences channel is talked about. A substance proprietor encodes the primary uncompressed picture utilizing a cryptographic key [26]. Using data concealing key the recipient can isolate additional data even the beneficiary has no information about the principal picture content [32]. Using the interpreting key the gatherer can remove data to get a picture like the first, however can't separate the supplementary data. In case the recipient has both the data concealing key and the cryptographic key, the gatherer can evacuate the supplementary data and the main picture with no disaster [33].

A novel plan procedure to reversibly conceal information into encrypted dim scale image in a divisible way [8]. Amid the principal stage, the substance proprietor performs image encryption by pixel permutation utilizing the encryption key [19]. The information hider then conceals a few information into the encrypted image by modifiable histogram based information hiding, constructing utilization of information hiding key. At the collector side, if the recipient has just encryption key, he can produce a image like the first one, yet can't examine the concealed information [25]. In the event that the collector has just information hiding key, he can separate the information, however can't read the substance of the image. On the off chance that the collector has both keys, he may first concentrate the information utilizing information hiding key and afterward decode the image utilizing cryptographic key [10]. Since the quality of the RDH system depends predominantly on three components - vigor, impalpability level in the stego image, and inserting limit [9]. The RDH framework leaves exceptional examples on the cover images and these examples accomplishments the steganalyst [10]. At the point when the measure of the sensitive message is little, the change space based systems, for example, DCT, DWT [15] and versatile RDH are not less inclined to steganalysis. In this procedure the contortion will be additionally less in light of the fact that implanting is performed in change space. All the above issues must be tended to while planning a RDH method which ought to be strong to assaults [23, 29]. We have to create RDH procedures where we can install information equivalent or more than

existing strategies and with no deformation in stego image so the sanctuary of the message can be enhanced [37, 40].

Information embedding away is the strategy by which a few information is covered up into a digital image. The information might be some content identified with the image, for example, confirmation information or creator data [6]. At the beneficiary side it must have the capacity to remove the hided information. In some high-exactness applications, for example, medicinal, military safety and remote detecting [21], it is exceptionally wanted that first image ought to be superbly recouped after information extraction [19]. An information hiding system fulfilling this prerequisite is known as reversible information covering up. They are likewise named as invertible, lossless or deformation free information hiding [27]. A large portion of the proposed information hiding plans is not reversible. Reversible information covering up should be possible from multiple points of view like, Integer-to-Integer Wavelet Transform, Difference extension, and Histogram change [26]. The principle objective of this work is to execute a Histogram moving (HS) based Reversible Data Hiding (RDH) strategy that can furnish a high inserting limit with least deformation [22, 36]. A substance proprietor takes the reverse s-request of the histogram. After that information hider conceals the extra information into the image utilizing information hiding key and afterward image encryption with the assistance of cryptographic key however the beneficiary does not think about the first substance [13, 18]. With an encrypted image containing extra information, a collector can just get the substance of the image after unscrambling it as per the cryptographic key, and afterward extricate the installed / entrenched information and recoup the first image as per the information hiding key [29]. In the plan, the information exclusion is Non-divisible from the substance unscrambling.

The examination point of information covering up is to expand the RDH limit and enhance the nature of stego images. A few creators proposed different novel and secure RDH strategy in light of Histogram Modification and Skew tent guide [12, 15, 19], Which comprises of image cryptography, information installing and information exclusion/image recuperation stages. In the first stage, The substance proprietor will takes the reverse s-request of the histogram [37, 39]. After that information hider will shroud the extra information into the image utilizing information hiding key and afterward performs image encryption with the assistance of key however the beneficiary does not think about the first substance [8, 18]. With an encoded image containing extra information, a collector can just get the substance of the image after decoding it as indicated by the encryption key, and after that concentrate the installed / embedded information and back in original form the first image as per the information hiding key [35, 37]. In the plan, the information extraction is non-divisible from the substance decoding [15]. Reversible information embedding away can be considered as an answer for trade data and news between individuals or associations around the globe over the Internet with no dread of the message being recognized and without loss of respectability of cover cover Image [20, 30]. Then again, there has been an extraordinary worry about protecting the licensed innovation privileges of computerized media, for example, content, image, sound, and video [12]. This has essentially inspired the enthusiasm for reversible data hiding strategies over the current years [5].

Reversible information hiding proselytes the sensitive data into a mixed code such that exclusive the expected beneficiary, who has the extraction key, can read this sensitive message [15]. Moreover, an outsider can confess that a sensitive message hosts been sent starting with one gathering then onto the next however he/she can't read this message [14]. In any case, reversible information hiding procedures shroud the very presence of this sensitive message. Accordingly, an outsider can't realize that a sensitive message has been installed / embedded inside a stego record or sent over a system [22, 33]. The execution of the information hiding techniques can be estimated by the consignment limit restrain, ocular eminence and multifaceted nature, where the ocular eminence is the nature of the stego watermarked image after the installing activity is completed, and many-sided quality is various scientific tasks, which depicts the calculation [16, 17]. Another grouping paradigm of information hiding plans is the real procedure of information inserting, among which the most widely recognized are: pressure, distinction development (DE) [4], histogram moving (HS) [17] and Histogram Modification (HM) [25]. With everything taken into account, inserting of sensitive message definitely will origin some deformation of the original image. It is profoundly attractive that this contortion be as little as could be expected under the circumstances while meeting different necessities, for example, adequate limit and strength [11]. Inspiration driving this examination work is to finish up the performed research, and goes about as an entire reference of the outcomes got so far [32]. We join the two plans i.e. HS and HM into one general information installing calculation and make longer it to the joint photographic specialists gathering (JPEG) design images [31]. Improved, the issue to be delivering in look into is to convey sensitive data to remote client over an uncertain channel. However while thinking about the barrier of cryptography, cryptographic methods can't be utilized to take care of the specific issue and the utilization of steganography [7, 17], as an elective arrangement, is investigated. Secure correspondence, can likewise be conceived into classifications and diverse classes of secure correspondence have distinctive necessity and issues [24]. The primary target of research is along these lines to think about the utilization of reversible information embedding away since it keeps up the amazing possessions that the first original image can be lossless [23] recouped after entrenched information is removed while securing the image substance's privacy. Reversible information covering up encourages secure correspondence in self-correspondence, balanced correspondence and one-to-numerous correspondence [34, 38].

Table 3. Comparison between data hiding techniques [14]

Techniques	**PSNR (dB)**	**Data Distortion**
Dissimilar Expansion based Reversible message embedding algorithm	48	High (Huge Data)
Reversible message development embedding techniques	55	Small (Tiny Data)
Data hiding using reversible order	42	Nothing
Encryption using Reversible separable data hiding	38	Nothing (Tiny data)
Pixel assortment, Error extension and adaptive prophecy based Reversible digital data Watermarking	49.3	High (huge data)
Side match based enhanced encrypted reversible data hiding	47	Small
Optimal binary codes based several reversible data hiding techniques	38	Small
Compressed Gray scale images encryption	39	Nothing
Images is embedded by Lossless data	43	Nothing
arrangement and prophecy based Reversible watermarking algorithm	47	extremely small

Table 4. Comparison between related works

Performance Indicator	**Peak Signal to Noise Ratio (PSNR) (DB)**	**Structural Similarity (SSIM)**
Ales Roceka et. al. [2]	81	0.999974
Chen Cui et. al. [5]	42.80	0.990
Chuan Qin et. al. [6]	56	0.99975
Chuan Qin et al. [7]	51.15	0.9995
Dalel Bouslimi et. al [8]	47.3	0.994
Diljith M. Thodi et. al [9]	52.5	0.9997
Frank Y. Shihet. Al. [11]	66.03	0.9998
Hwai-Tsu Hu et. al. [13]	40.48	0.973
Kede Ma et. al. [15]	67.16	0.99985
Manas Ranjan Nayak et. al. [17]	44.77	0.991
Sudhanshu Suhas Gongea et. al. [21]	55.16	0.9978

Thai-Son Nguyen et. al. [22]	83.54	0.9999
Thien Huynh et. al. [23]	49.38	0.994
Vasiliy Sachnev et. al. [24]	59.23	0.9979
Xiang-yang Wang et. al. [28]	42.93	0.899
Xiaochun Cao et. al. [29]	48.26	0.992
Xiaolong Li et. al. [30]	63.88	0.9992
Xiyao Liua et. al. [33]	63.09	0.9995
Yahya AL-Nabhani et. al. [34]	68.27	0.9996
Yongjian Hu et. al. [35]	46.03	0.991
Yu-Chi Chen et. al [36]	39.85	0.500
Yunpeng Zhang et. al [37]	90.56	0.9881
Yusuf Perwej et. al. [38]	58.42	0.9965

3. CONCLUSION

In this paper, a widespread review of reversible and non reversible data hiding techniques are described briefly. All data hiding techniques like water marking, cryptography and steganography are analyzed and compared on the basis of some parameters like PSNR and SSIM. The performance and comparison of these methods are represented in a table. So researchers can be enhanced their capacities of selecting the best suited data hiding approaches for secret communication. Separable and non separable data hiding techniques are also used for confidential and authenticated communication in digital media environment. The existing techniques are improved by using combination of steganography and cryptography.

4. REFERENCES

[1] A. Rasmi, and M. Mohanapriya, "An Extensiv Survey of Data Hiding Techniques", European Journal of Applied Sciences, Volume 9 (3), pp. 133-139, 2017.

[2] Ales Roceka, Karel Slavícekb, Otto Dostálb, and Michal Javorník, "A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters", Biomedical Signal Processing and Control, Elsevier, Volume 29, pp. 44-52, 2016.

[3] Anoop Kumar Chaturvedi and Piyush Kumar Shukla, "Reversible Data-Hiding Schemes For Encrypted Image: A Review", International Journal of Advanced Research in Computer Science, Volume 8, (8) pp. 658-660, 2017.

[4] C. Munuera, "Steganography and error-correcting codes", Signal Processing, Elsevier, Volume 87, pp. 1528–1533, 2007.

[5] Chen Cui, and Xia-Mu Niu, "A robust DIBR 3D image watermarking algorithm based on histogram shape", Measurement, Elsevier, Volume 92, pp. 130–143, 2016.

[6] Chuan Qin, and Xinpeng Zhang, "Effective reversible data hiding in encrypted image with privacy protection for image content", J. Vis. Commun. Image R., Elsevier, Volume 31, pp. 154–164, 2015.

[7] Chuan Qin, Huili Wang, Xinpeng Zhang, and Xingming Sun, "Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode", Information Sciences, Elsevier, Volume 373, pp. 233–250, 2016.

[8] Dalel Bouslimi, and Gouenou Coatrieux, "A crypto-watermarking system for ensuring reliability control and traceability of medical images", Signal Processing: Image Communication, Elsevier, Volume 47, pp.160–169, 2016.

[9] Diljith M. Thodi and Jeffrey J. Rodríguez, "Expansion Embedding Techniques for Reversible Watermarking", IEEE Transactions on Image Processing, Volume 16,(3), pp. 721-730, 2007.

[10] Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn, "Information Hiding—A Survey", Proceedings of the IEEE, Volume 87, (7), pp.1062-1078, 1999. (Publisher Item Identifier S 0018-9219(99)04946-4.)

[11] Frank Y. Shih, and Xin Zhong, "High-capacity multiple regions of interest watermarking for medical images", Elsevier on Information Sciences, Volume 367-368, pp-648-659, 2016.

[12] Huaiqing Wang and Shuozhong Wang, "Cyber Warfare: Steganography vs. Steganalysis", Communications of the ACM, Volume 47,(10), pp. 76-82, 2004.

[13] Hwai-Tsu Hu, Jieh-Ren Chang, and Ling-Yuan Hsu, "Robust blind image watermarking by modulating the mean of partly sign-altered DCT coefficients guided by human visual perception", Int. J. Electron. Commun. (AEÜ), Elsevier, Volume 70, pp. 1374–1381, 2016.

[14] Jitha Raj.T, and E.T Sivadasan, "A Survey Paper on Various Reversible Data Hiding Techniques in Encrypted Images", International Advance Computing Conference (IACC), IEEE, pp-1139-1143, 2015.

[15] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", IEEE Transactions on Information Forensics and Security, Volume 8,(3), pp. 553-562, 2013.

[16] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", IEEE Transactions on Information Forensics and Security, Volume 8,(12), pp. 1947-1960, 2013.

[17] Manas Ranjan Nayak, Joyashree Bag, Souvik Sarkar, and Subir Kumar Sarkar, "Hardware implementation of a novel water marking algorithm based on phase congruency and singular value decomposition technique", Int. J. Electron. Commun. (AEÜ), Elsevier, Volume 71, pp. 1–8, 2017.

[18] Minati Mishra, Priyadarsini Mishra and Flt. Lt. Dr. M.C. Adhikary, "Digital Image Data Hiding Techniques: A Comparative Study", ANSVESA, Volume 7, (2), pp.105-115, 2012.

[19] Po-Chyi Su, Tien-Ying Kuo, and Meng-Huan Li, "A practical design of digital watermarking for video streaming services", J. Vis. Commun. Image R., Elsevier, Volume 42,(C), pp. 161–172, 2017.

[20] Shrinivas Khadare and Urmila Shrawankar, "Image bit depth plane digital watermarking for secured classified image data transmission", International Conference on Information Security & Privacy (ICISP 2015), Procedia Computer Science, Elsevier, Volume 78, pp. 698-705, 2016.

[21] Sudhanshu Suhas Gongea, and Ashok Ghatol, "Aggregation of Discrete Cosine Transform Digital Image Watermarking with Advanced Encryption Standard Technique", Twelfth International Multi-Conference on Information Processing, Procedia Computer Science, Elsevier, Volume 89, pp. 732 – 742, 2016.

[22] Thai-Son Nguyen, Chin-Chen Chang, and Xiao-Qian Yang, "A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain", Int. J. Electron. Commun. (AEÜ), Elsevier, Volume 70,(8), pp. 1055–1061, 2016.

[23] Thien Huynh, Oresti Banos, Sungyoung Lee, Yongik Yoon, and Thuong Le-Tien, "Improving digital image watermarking by means of optimal channel selection", Expert Systems With Applications, Elsevier, Volume 62, pp. 177–189, 2016.

[24] Vasiliy Sachnev, Hyoung Joong Kim, Member, Jeho Nam Senior Member, Sundaram Suresh, and Yun Qing Shi, "Reversible Watermarking Algorithm Using Sorting and Prediction", IEEE Transactions on Circuits and Systems for Video Technology, Volume 19,(7), pp. 989-999, 2009.

[25] Wang Chun-peng, Wang Xing-yuan, Xia Zhi-qiu, Zhang Chuan, and Chen Xing-jun, "Geometrically resilient color image zero-watermarking algorithm based on quaternion Exponent moments", J. Vis. Commun. Image R., Elsevier, Volume 41, pp. 247–259, 2016.

[26] Wioletta Wójtowicz, and Marek R. Ogiela, "Digital images authentication scheme based on bimodal biometric watermarking in an independent domain", J. Vis. Commun. Image R., Elsevier, Volume 38, pp. 1-10, 2016.

[27] Xiang-yang Wang, Yu-nan Liu, Meng-meng Han, and Hong-ying Yang, "Local quaternion PHT based robust color image watermarking Algorithm", J. Vis. Commun. Image R., Elsevier, Volume 38, pp. 678-694, 2016.

[28] Xiang-yang Wang, Yu-nan Liu, Huan Xu, and Ai-long Wang, Hong-ying Yang, "Blind optimum detector for robust image watermarking in nonsubsampled shearlet Domain", Information Sciences, Elsevier, Volume 372, pp. 634-654, 2016.

[29] Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, and Xiaojie Guo, "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation", IEEE Transactions on Cybernetics,Volume 46,(5), pp-1132-1143, 2016.

[30] Xiaolong Li, Weiming Zhang, Xinlu Gui, and Bin Yang, "Efficient Reversible Data Hiding Based on Multiple Histograms Modification", IEEE Transactions on Information Forensics and Security, Volume 10,(9), pp. 2016-2027, 2015.

[31] Xinpeng Zhang, Member, "Reversible Data Hiding With Optimal Value Transfer", IEEE Transactions on Multimedia, Volume 15,(2), pp. 316-325, 2013.

[32] Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image", IEEE Signal Processing Letters, Volume 18,(4), pp.255-258, 2011.

[33] Xiyao Liua, Fangfang Lia, Jingyu Dua, Yang Guanc, Yuesheng Zhuc, and Beiji Zoua, "A robust and synthesized-unseen watermarking for the DRM of DIBR-based 3D video", Neurocomputing, Elsevier, Volume 222, pp. 155-169, 2017.

[34] Yahya AL-Nabhani, Hamid A. Jalab, Ainuddin Wahid, and Rafidah Md Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural Network", Journal of King Saud University – Computer and Information Sciences, Elsevier, Volume 27,(4), pp. 393–401, 2015.

[35] Yongjian Hu, Heung-Kyu Lee, Kaiying Chen, and Jianwei Li, "Difference Expansion Based Reversible Data Hiding Using Two Embedding Directions", IEEE Transactions on Multim edia, Volume 10,(8), pp. 1500-1512, 2008.

[36] Yu-Chi Chen, Chih-Wei Shiu, and Gwoboa Horng, "Encrypted signal-based reversible data hiding with public key Cryptosystem", J. Vis. Commun. Image R., Elsevier, Volume 25, (5), pp. 1164-1170, 2014.

[37] Yunpeng Zhang, Chengyou Wang, Xiaoli Wang and Min Wang, "Feature-Based Image Watermarking Algorithm Using SVD and APBT for Copyright Protection", Future Internet, MDPI, Volume 9,(2), 13, pp-1-15, 2017.

[38] Yusuf Perwej, Firoj Parwej, and Asif Perwej, "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection", The International Journal of Multimedia & Its Applications (IJMA), Volume 4,(2), pp. 21-38, 2012.

[39] Zhenghui Liu, FanZhang, JingWang, HongxiaWang, and JiwuHuang, "Authentication and recovery algorithm for speech signal based on digital watermarking", Signal Processing, Elsevier, Volume 123, pp. 157–166, 2016.

[40] Zhuhong Shao, Yuanyuan Shang, Rui Zeng, Huazhong Shu, Gouenou Coatrieux, and Jiasong Wu, "Robust watermarking scheme for color image based on quaternion- type moment invariants and visual cryptography", Signal Processing:ImageCommunication, Elsevier, Volume 48, pp. 12–21, 2016.

5. AUTHORS PROFILE

Anoop Kumar Chaturvedi: Obtained his Bachelor's degree from Dr. H.S. Gour University, Sagar, India in 1998 and Master's degree in Computer Science & Engineering with gold medal from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India in 2010. He is currently pursuing his Ph.D. degree in Computer Science & Engineering at Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India. His research interest includes digital watermarking and image data hiding.

***Dr*. Piyush Kumar Shukla:** Received his Bachelor's degree in Electronics & Communication Engineering, LNCT, Bhopal in 2001, M.Tech (Computer Science & Engineering) in 2005 from SATI, Vidisha and Ph.D. (Computer Science & Engineering) in 2013 from RGPV, Bhopal. M.P. India. He is Member of ISTE (Life Member), IEEE, IACSIT, IAENG. Currently he is working as an Assistant Prof. in Department of Computer Science & Engineering, UIT-RGPV Bhopal. He is also I/C of PG Program (Dual Degree Integrated PG-Programs) in DoCSE, UIT, RGPV, Bhopal, Madhya Pradesh, Bhopal. He has published more than 40 Research Papers in various International & National Journals & Conferences including 04 Papers in SCIE Journals & More than 05 papers in Scopus Journals.