

Video Steganography using Mid-Point Circle Algorithm and Spatial Domain Technique

M.Mary Shanthi Rani¹, S.Lakshmanan² and G.Deepalakshmi³

¹Assistant Professor, Department of Computer Science and Applications,
The Gandhigram Rural Institute – Deemed to be University, Tamil Nadu, India

²Research Scholar, Department of Computer Science and Applications,
The Gandhigram Rural Institute – Deemed to be University, Tamil Nadu, India

³M.Phil Scholar, Department of Computer Science and Applications,
The Gandhigram Rural Institute – Deemed to be University, Tamil Nadu, India

Abstract:

Recent advances in information innovation have made quick delivery and sharing of interactive media information possible. In any case, these advances in innovation are leading breaches to information security and personal information. Nowadays, it is exceptionally dangerous to deal with the information on the web against hackers. Researchers are exploring new techniques for concealing message as well as concealing the presence of message. Steganography is the way toward concealing secret information inside an information source which is referred as a cover medium. Steganography has applications in various fields, like medical field, military etc. It is mainly utilized as a part of circumstances where the privacy of data is of prime significance in correspondence. Different types of steganography are introduced based on the sort of cover medium like sound, video, content, picture etc. Video Steganography is the procedure in which message is embedded inside the video kind of cover medium in such manner that is existence. In this paper, Mid-point circle algorithm is used with LSB technique to enhance the efficiency of the embedding process with low distortion .

Keywords — Steganography, Spatial domain technique, Least Significant Bit, Midpoint Circle, PSNR, MSE.

I. INTRODUCTION

This Computer security, also known as cyber security or IT security is the safeguard of computer systems from the theft or spoil to the hardware, software or the information, as well as from interruption or misdirection of the services they provide. Recent advances in information technology have made quick release and sharing of multimedia information is possible. Now days, it is very unsafe to handle the data in internet against intruders. Data is generally in the form of text, audio, video and image. The two types of information security technique are Cryptography and Steganography [1].

The principle reason for Cryptography is to enhance Confidentiality, Integrity, Non-repudiation and Authentication. The operation of a cipher usually depends on a piece of auxiliary information, called a key. The encoding method is differed relying upon the key, which changes the itemized operation of the algorithm. A key must be chosen

before utilizing a figure to scramble a message [2]. Without information of the key, it is to a great degree troublesome, if certainly feasible, to decode the subsequent cipher text into readable plaintext.

"Steganography" originates from "Greek". The word stego implies cover and grafia implies writing which signifies "Covered writing" [3]. Steganography aims at hiding the existence of the authentic communication. Steganography has developed into one of the most robust and efficient methods to send secret or sensitive data to another party without the knowledge of any interceptor.

In steganography, the sender uses usual file like video, image, audio and text known as cover file which would appear to be of no importance to any interceptor. Video Steganography is defined as the art and science of embedding secret data into videos. A video file is a set of frames (still-images) [4]. Some techniques hide data in the individual frames of the video which is known as video steganography as the extension of image steganography.

Video Steganography refers to the process of hiding the information into video. This method not only hides the data, but also it converts the original data into secret code. The performance of steganography techniques are assessed based on the following metrics.

Imperceptibility refers to the visibility of alteration inside the cover media. High Imperceptibility means rising the invisibility of minor modifications in cover object. Modern day Steganalysis approaches are highly intellectual to detect minor modifications [5].

Payload or capacity refers to the quantity of secret message that can be hidden inside cover media. Video are in very popular as highly used cover media object due to high embedding capacity and embedding efficiency.

The attacks or methods functional in stego object to extract hidden or secret data are known as statistical attack .Steganography algorithm should be rigid against robust and statistical attacks. It describes robustness characteristic.

The most significant feature of any steganographic algorithm is security. The embedding method should have high security with the least amount of weakness to attacks. Several approaches are projected to secure message in steganography. Data hiding and Data retrieval are two parameters used in analyzing the computational cost of steganography approach. Data hiding required embedding data within a cover video frame and data recovery refers to extraction of secret message from the stego frame. Increment in embedding capacity may also guide to degradation of video quality or degradation of the original contents of video [6]. Video steganography technique must control degradation of video quality. Robustness refers to the capability of the steganography technique to retain the hidden message after many image related operations, like compression, cropping, rotation and filtering etc.

Steganography technique can be classified into six types: Spatial domain techniques, Transform domain techniques, Spread spectrum Technique, Statistical method, Distortion technique and Cover Generation Methods. In this paper; we focused on spatial domain techniques. These algorithms are

primarily classified into two categories based on whether the pixels of the image are modified directly or some mathematical transform is applied on the images before embedding [7]. The former techniques are called spatial domain techniques. Spatial domain technique is a simple method in which the secret information is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during data hiding a data [8]. Least significant bit (LSB)-based steganography is one of the easiest techniques. Least significant bit of the pixels of the cover images is replaced by the bits of secret information. Replacing few least significant bits of the pixels do not make a significant visual change in the image. Since the change is less it is invisible to the human visual system. In the meantime, if a hacker suspects the presence of the message, at that point he can follow the message without much trouble by gathering all the least significant bits of the pixels from the image [9]. Spatial domain Techniques are classified into different categories [10]:

1. Pixel Value Differencing (PVD).
2. Most Significant Bit (MSB).
3. Least Significant Bit (LSB).
4. Quantization Index Modulation (QIM).
5. Random Pixel Embedding (RPE).

This method, LSB is used as it is very effective to hide the secret file in any file.LSB method is also known as 8th bit modification method as it uses 8th bit of every byte in a pixel to hide a bit of the secret message. In a grayscale image each pixel is of 8 bits, there are 256 possible values of pixels. In LSB, the pixel value is changed without noticeable change to human visual perception [11]. Digital color images are usually stored in 24-bit files and use the RGB (Red, Green, and Blue) color model. Each pixel is represented by 256 different color values of Red, Green and Blue. For example the RGB color pixel values in 24 bit image can be as follows:

```
(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)
```

When the letter A, with binary representation is 01000100 is embedded into the Least Significant

Bits of this part of the image, the resulting grid is as follows:

```
(00101100 00011101 11011100)
(10100110 11000100 00001101)
(11010010 10101100 01100011)
```

Although the letter was embedded into the first 8 bytes of the grid, only the 2 highlighted bits need to be changed according to the embedded message. On average only some part of the bit in an image will need to be customized to hide a secret message using the maximum cover size..

II. RELATED WORK

Mary Shanthi Rani et.al [12] has developed a system for hiding stego images inside the Visual Cryptography VC shares which are meaningless and cannot be deducted by Steganalysis tools. VC and Steganography play a role in information security. This proposed method incorporates these two technologies for providing multilevel multimedia security, so that secret message can be transmitted over the network confidently. The algorithm is tested with text and image files. The results establish that the quality of the recovered image and message is same as that of the original image. Any digital data can be transmitted in a secured way using this scheme. More amounts of data can be transmitted by increasing the quantity of VC shares. Since the stego image is hidden in the spatial domain of the VC shares, it is prone to transform domain attacks. To overcome, this work can be extended to hide the data in the frequency domain of the shares.

P.Thiyagarajan et.al [13] proposed design based 3D Image steganography in which they test the various attacks such as cropping, rotation, scaling etc. The algorithm re-triangulates a part of triangle mesh and the secret message is embedded into the new positions in vertices. Up to 9 bits of information can be implanted into a vertex of the triangle without causing any progressions to the geometrical structure and visibility of the original 3D image.

A novel approach for secret communication by consolidating the ideas of Steganography and QR codes has been proposed by Mary Shanthi Rani [14]. The suggested strategy includes two phases: (i) Encrypting the message by a QR code encoder and

in this manner making a QR code (ii) Hiding the QR code inside a color image. This hiding process embeds the quantized QR code so that it will not make any visible distortion in the cover image and it introduces very minimum Bit Error Rate (BER). The experimental result demonstrates that the proposed strategy has high imperceptibility, integrity and security.

Weiqi Luo et.al [15] proposed a method that embeds the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges. In this method, different kinds of Steganalysis algorithms are used in natural image and it is observed that both visual quality and security of stego images are enhanced using LSB-based approaches and their edge adaptive versions.

Mary Shanthi Rani et.al [16] has proposed a new approach that data hiding and compression in medical images. This method gives the better performance with low computation complexity and ensures fast and secure transmission of medical images. As Run length coding lossless compression is used, the retrieved image by the receiver is the same as the original image sent by the sender.

D. Battikh, et.al [17] proposed an improvement of the message security of adaptive data hiding in edge areas of images with spatial Low Significant Bit domain systems. The improvement consists by using an efficient chaotic system to choose in pseudo-chaotic manner, the pixels in the cover image where the bits of secret information are embedded. In this way, the inserted message becomes secure against message recovery attacks

N Sathisha et.al [18] proposed Spatial Domain Steganography with 1-Bit Most Significant Bit (MSB) in a chaotic manner. The cover image is decomposed into 8*8 matrix blocks of equal size. The first block of the cover image is embedded into 8 bits of upper and lower bound values if necessary for retrieving payload at the destination. The mean of median values and difference between successive pixels is determined to embed payload in 3 bits of Least Significant Bit (LSB) and one bit of Most Significant Bit (MSB) in a chaotic manner. The capacity and security is improved and compared to the existing methods with reasonable PSNR.

A new strategy for VC validation is proposed in [19], by embedding QR Code in a non-area of interest of the secret image without affecting its quality. The novelty of the proposed method is multifold. In the first place, the secret image is authenticated by embedding QR Code. The volume of a secret message transmitted has been considerably inversed, as VC shares that hide the secret image additionally hides secret message embedded in QR Code. Third, security and efficiency of transmission of VC shares are upgraded by performing lossless compression. This is a way to solve the problem of pixel expansion of VC shares. Despite the fact that this framework improves the security of VC shares, there are few hindrances. Dissimilar to general VC frameworks that do not require any computation at the receiver, this method executes decompression algorithm at the receiver. This algorithm of the embedded QR Code is just connected to (2, 2) VC.

Pooja Yadav et.al [20] proposed a method that hides a secret video stream in cover video stream. Each frame of secret video will be split into individual components which are further converted into 8-bit binary values, and encrypted by XOR operation with a secret key. Encrypted frames are hidden in the Least Significant Bit (LSB) of each frame using sequential encoding of Cover video. To improve more security, each bit of secret frames will be stored in cover frames following a pattern BGRRGBGR. The visual quality of the video stream is not affected much and the secret video is easily recovered.

Divya et.al [21] proposed to apply optimization to hide the secret data messages effectively within cover images to ensure more hiding capacity, good security, distortion less transmission and effective recovery of the hidden messages without corruption. The optimization scheme is Particle Swarm Optimization that provides the best pixel positions in the cover image that can be used to embed the secret message bits so that less image distortion occurs.

Mary Shanthi Rani et.al [22] have proposed another approach consolidating visual cryptography and steganography methods for giving multi-level multimedia security. Some novel message concealing methods in RGB Domain are exhibited.

Uma sahu et.al [23] proposed a method for hiding data in a video in which random sequence generator is used for random frame selection and pixel swapping operation randomly. In this proposed method, random frame selection and pixel swapping operation with the help of key1 and key 2. It makes this algorithm very secure even after using the simple LSB embedding method for message bit insertion.

III. PROPOSED METHOD

A Various kinds of video steganography methods are introduced recently due to increase in the number of video application. In this paper, we have proposed Least Significant Bit (LSB) Technique for Video Steganography, which performs insertion of text in selected frames. Furthermore, the proposed method embeds secret message in positions selected by mid-point circle method. The proposed video steganography is divided into some phases.

A. Phase I - Selection of Frames in Cover Video

In this Video Steganography we are using AVI (Audio Video Interleave). The information of the cover video (AVI) such as number of frames (n), frames speed (fp/sec), frame height (H) and the width (W) are extracted from the cover video. The number of frames for hiding data is selected using prime number method. This is done by selecting the middle prime number from the list of prime numbers within the limit of total number of frames.

B. Phase II - Secret message

The secret text message is changed into ASCII values which are further converted into binary bits. These binary bits are hidden at the fixed locations using Mid Point Circle algorithm. It using N Dimension of RGB channel, we store the secret message into Red channel in the selected frames. The binary bits are embedded using LSB algorithm in spatial domain technique.

C. Phase III - Data Embedding

The secret message is embedded in a pixel image by using (LSB) Least Significant Bit method which archives minimum distortion. The correct positions of the pixel are found out using Midpoint Circle

algorithm for embedding secret text message bits. The frame with embedded secret message is called stego frame and this process is repeated for all selected frames.

Mid-point circle algorithm is used to determine the points needed for rasterizing a circle.

ALGORITHM:

1. Input radius r and circle center (x_c, y_c) , and obtain the first point on circle centered at original $(x_0, y_0) = (0, r)$
2. Calculate initial decision parameter

$$p_0 = \frac{5}{4} - r$$
3. At each X_k position, starting at $k=0$, perform the test:
 If $p_k < 0$, the next point along the circle centre at $(0,0)$ is (x_k+1, y_k)

$$(i, e) \quad P_{k+1} = p_k + 2x_{k+1} + 1$$
 Otherwise, the next point along circle is (x_k+1, y_k-1)

$$P_{k+1} = p_k + 2x_{k+1} + 1 - 2y_{k-1}$$
 Where $2x_{k+1} = 2x_{k+2}$, and $2y_{k+1} = 2y_{k-2}$.
4. Determine symmetry points on the other seven octants.
5. Move each calculated pixel position (x, y) in to circle path centered at (x_c, y_c) as $x = x + x_c, y = y + y_c$
6. Repeat the steps 3 and 5 until $x \geq y$.

ALGORITHM:

Steps for encoding process:

1. Input cover video file
2. Read the information about cover video.
3. Convert the video into frames
4. Select the middle prime number frame to embed the secret message.
5. Using Mid Point Circle algorithm, identify the positions in this frame to embed data bits into red channel.
6. Repeated values are left out and LSB method is used to embed the secret message in the selected positions in a frame, creating the stego frame.
7. Stego frames are combined with other frames to create stego video.

Steps for decoding process:

1. Input stego video file.
2. Convert the stego video file into frames.

3. Identify the stego frames and apply the Least Significant Bit (LSB) method to extract the hidden message from the red channel of the frame.

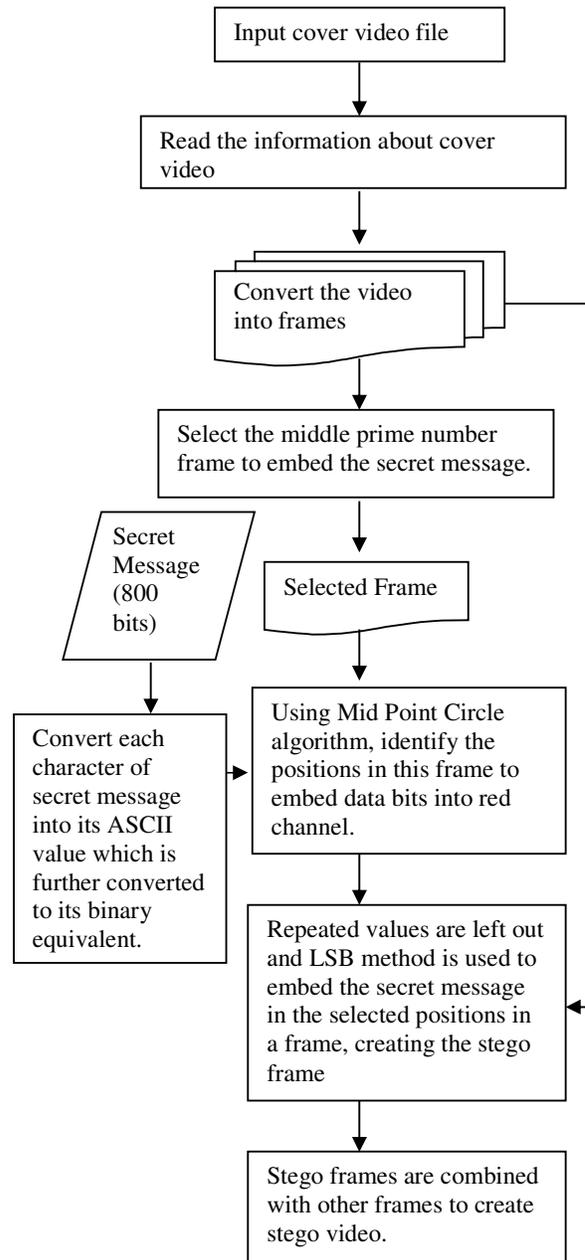


Fig. 1 Flow chart of Encoding Process

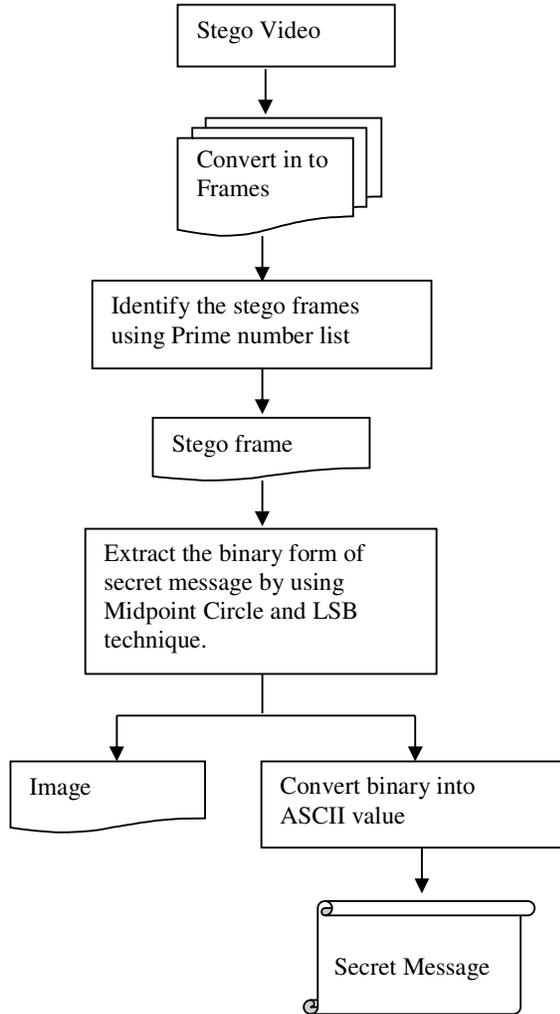


Fig. 2 Flow chart of Decoding Process

IV. RESULT AND DISCUSSION

Audio Video Interleave (AVI) files are used to analyze the performance of the proposed method. All videos contain high pixel resolution at F frames per second, and a data rate of P kbps. Each cover video contains N frames. In all video frames, the secret message appears as a large text message split into bits, at the locations of pixels in RGB components of cover frame. The resolution, frame rate and number of frames in all four AVI video files considered for result analysis.

Performance Metrics

To measure the imperceptibility of steganography techniques, several metrics are used. The metrics indicate how similar or differentiate the stego image

is from cover image. The following metrics are used:

Mean Square Error (MSE) is computed by performing byte by comparing between the cover image and stego image. The Computation formula is expressed as.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [A(i, j) - Y(i, j)]^2 \quad \dots(1)$$

M: Numbers of rows of cover image

N: Number of column of Cover Image

A_{ij}: Pixel value of cover Image

Y_{ij}: Pixel value of Stego Image

Higher value of MSE indicates variation between Cover image and Stego image.

Peak signal to noise ratio (PSNR) measures in noise of the quality of the stego image compared with the cover image. The highest PSNR value is better quality. PSNR is evaluated by using of this equation.

$$PSNR = 10 \log_{10} \left(\frac{Max(A)^2}{MSE} \right) \quad \dots(2).$$

TABLE I PERFORMANCE ANALYSIS OF THE PROPOSED METHOD

Cover Video Frames	Stego Video Frames	Capacity of Text Data	PSNR	MSE
		800 bits	82.0468	0.0004
		800 bits	81.9556	0.0004
		800 bits	74.6185	0.0023

The proposed algorithm is applied to four video files and the performance analysis is tabulated in Table1. From Table 1, it is observed that flower video file has achieved the highest PSNR value 82.0468 even after the embedding data. It is also obvious from Table I that all video files achieve PSNR value greater than 70 which represent good

quality. Then another video files are Rhino PSNR value 81.9556 and the Xholophone video file PSNR value 74.6185.

TABLE III COMPARATIVE ANALYSIS OF LSB METHOD

Video File	Capacity of Text Data [22]	PSNR(db)		MSE	
		Existing method [23]	Proposed	Existing method [23]	Proposed
Rhino.avi	1Kb	66.29	81.96	0.5220	0.0004
Akivo.avi	1Kb	64.11	81.67	0.6572	0.0004

Table II reveals the superiority of the proposed method for embedding 1 kb of secret data by achieving 20db higher than the similar existing method.

V. CONCLUSION

A new Video steganographic method is proposed in this paper. It works directly on the frames in the video and selects the frame to embed the secret message. The frame selection is the important criteria in the proposed structure. The image thus embedded using the LSB Algorithm, saves the efficiency of the video. Since, least significant bit is selected to hide the intruder is unaware of the data inside the video. This algorithm provides high capacity and imperceptible stego-image for human vision of the hidden secret information. The performance of the steganography algorithm is studied and experimental results show that this method can be applied on videos with no visible degradation in its quality.

REFERENCES

1. C.P.Sumathi, T.Santanam and G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding", *International Journal of Computer Science & Engineering Survey (IJCSSES)*, Vol.4, No.6, December 2013.
2. M.Mary Shanthi Rani, G. Germine Mary and K. Rosemary Euphrasia, "High level Multimedia Security by incorporating Steganography and Visual Cryptography", *International Journal of Innovations & Advancement in Computer Science IJIACS - ISSN 2347 – 8616 Vol.4, Special Issue September 2015*.
3. M. Mennattallah. Sadek, Amal S. Khalifa Mostafa and G. M. Mostafa "Robust video steganography algorithm using adaptive skin-tone detection", *Springer Multimed Tools Applications*, Vol.76, Issue.2, pp.3065-3085, 2017.
4. Deepali Singla and Mamta Juneja, "An Analysis of Edge Based Image Steganography Techniques in Spatial Domain", *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, Chandigarh,India, pp.1-5 March, 2014.
5. Mansi Dave and HinalSomani, "A survey on digital video steganography techniques used for secure transmission of data", *International Journal of Advance Research and Innovative Ideas in Education*, Vol.2, Issue.6, pp.479-485, 2016.
6. Swetha V, Prajith V and Kshema V, "Data Hiding Using Video Steganography - A Survey", *International Journal of Computer Science Engineering and Technology*, Vol.5, Issue.6, pp.206-213, June 2015.
7. M. Mary Shanthi Rani and K.Rosemary Euphrasia , "Dynamic Hiding of message in RGB Domain based on Random Channel Indicator", *International Journal of Applied Engineering Research*, Vol.10, Issue.76, pp.478-483, 2015.
8. Ravneet Kaur and Bhavneet Kaur, "A Study and Review of Techniques of Spatial Steganography", *International Journal of Science and Research*, Vol.4, Issue.4, April 2015.
9. K.Rosemary Euphrasi and M. Mary Shanthi Rani, "A Comparative Study On Video Steganography in Spatial and IWT Domain" *IEEE International Conference on Advances in Computer Applications (ICACA) Coimbatore, India*,pp.104-109, 2016.
10. Alaa Fkirin, Gamal Attiya and Ayman El-Sayed, "Steganography Literature Survey, Classification and Comparative Study", *Communications on Applied Electronics (CAE)*, Vol.5, Issue.10, pp.13-22, September ,2016

11. Anil Khurana and B. Mohit Mehta, "Comparison of LSB and MSB based Image Steganography", *International Journal of Computer Science and Technology*, Vol.3, Issue.3, pp.870-871, July - Sept 2012.
12. M.MaryShanthi Rani, G.Germine Mary and K.RosemaryEuphrasia "Multilevel multimedia security by Integrating Visual Cryptography and Steganography Techniques", *Computational intelligence, Cyber Security and Computational Models. Advances in Intelligent Systems and Computing*, vol.412, pp.403-412, December, 2105.
13. P. Thiyagarajan, V. Natarajan, G. Aghila,V. PrasannaVenkatesan and R. Anitha, "Pattern Based 3D Image Steganography", *3D Research*, Springer, Vol.4, Issue.1, pp.1-8, 2013.
14. M.MaryShanthiRani and K.RosemaryEuphrasia, "Data Security Through QR Code Encryption and Steganography", *Advanced Computing: An International Journal (ACIJ)*, Vol.7, Issue.1/2, pp.1-7, March 2016.
15. Weiqi Luo, Fangjun Huang and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", *IEEE transactions on information forensics and security*, vol.5, issue.2, pp.201-214, June 2010.
16. M.Maryshanthi Rani and S.Lakshmanan "An Integrated Method of Data Hiding and Compression of Medical Images" *International Journal of Advanced Information Technology (IJAIT)*, Vol.6, Issue.1, pp.43-51, February 2016.
17. D. Battikh, S. El Assad, B. Bakhache, O. Deforges and M. Khalil, "Enhancement of two spatial steganography algorithms by using a chaotic system: comparative analysis" *IEEE 8th International Conference for Internet Technology and Secured Transactions*, London, UK, pp.20-25, December, 2013.
18. N Sathisha, Madhusudan G N, Bharathesh S, K Suresh Babu, K B Raja and Venugopal K R, "Chaos based Spatial Domain Steganography using MSB" *IEEE 5th International Conference on Industrial and Information Systems*, Mangalore, India, pp.177- 182, July 2010.
19. M.MaryShanthi Rani and G.Germine Mary, "Compression of VC Shares", *International Journal of Computational Science and Information Technology (IJCSITY)*, Vol.4, Issue.1, pp.57-65, February 2016.
20. Pooja Yadav, Nishchol Mishra and Sanjeev Sharma "A Secure Video Steganography with Encryption Based on LSB Technique" *IEEE International Conference on Computational Intelligence and Computing Research*, Enathi, India, pp.1-5, 2013.
21. E Divya and P Raj Kumar, "Steganographic Data Hiding using Modified APSO", *International Journal of Intelligent Systems and Applications (IJISA)*, Vol.8, Issue.7, pp.37-45, 2016.
22. M.Mary Shanthi Rani and S.Lakshmanan "Region Based Data Hiding in Medical Images" *International Journal of Advanced Research in Computer Science*, Vol.8, Issue.3, pp.1103-1107, March-April 2017.
23. Uma Sahu and Saurabh Mitra "A Secure Data Hiding Technique Using Video Steganography" *International Journal of Computer Science & Communication Networks*, Vol.5, Issue. 5, pp. 348-357, 2015.