IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 2, February 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

An Innovative Methodology of Steganography and Cryptography Elicited from Randomization and Base64 Code in GIF images

Dr. Vani Perumal[1]

[1] IT Department, Rustaq College, Ministry of Higher Education,
Al Rustaq, Sultanate of Oman

Abstract

India is ranked as the third country universally among the highest detected cyber threats says the Director of Enterprise Security Product Management of Symantec Corporation. Thus our country is in high risk in the cyber world. Hence security and protection are imperative features to be encompassed in the same. This paper proposes a combination of pioneering techniques such as steganography, cryptography and randomization to attain a high level of security by hiding any secret information in a GIF image. This procedure is instigated by selecting the correct GIF image. After selecting, the same GIF image is converted into frames. The secret information to be embedded is initially encrypted. Then from the generated frames, specific frame is selected and that image is converted as Base64 code and from that code, a specific line is also selected and the encrypted text is embedded. Then decrypted text is extracted from the GIF.

Keywords: *GIF, Frames, Randomization, Base64, Cryptography, Steganography.*

1. Introduction

Information is the principal wealth of all organization. Since cyber-attacks are growing in prominence every day, there is a core need to protect these information from the attacks while transmission. Steganography is the method of disguising a file, message, image, or video in another file, message, image, or video.

In this paper, the information need to be protected is disguised into a GIF file. First the GIF image is converted into frames. Then any of these frames are randomly selected for hiding the secret information. Before hiding the secret information, it is encrypted using Vigenere Cipher algorithm. After that this cipher text is embedded into a randomly selected lines of the equivalent frame's Base64 code. While extracting the original secret information, the Stego-GIF image is again converted back into frames and from those specific frames' equivalent Base64 code, the cipher text is extracted. Finally the cipher text is decrypted to get back the original secret information. Here multi-level security is implemented to protect that particular piece of information.

2. The Embedding Methodology

This section is dedicated to explain the procedure of embedding the secret information into the GIF image. This also gives the details of all the algorithms and methods used in creating a Stego-image.

2.1 Converting GIF image into frames

This is the initial step involved in GIF Steganography. Initially the GIF image is converted into various number of frames. The selection of number of frames are varied from one GIF to another GIF. The total number of frames to be converted from the GIF are based on animation involved in that particular image. The image which is given in this paper is converted into 124 different frames. The following figure named Fig. 1 shows some set of frames in a selected GIF image.

2.2 Randomization in Selecting Frames

The next step is randomization of frames. Once the GIF is converted into frames then from the set of available frames, some specific frames must be selected randomly for embedding secret information. To generate random numbers, PCG – Permuted Congruential Generator algorithm can be used. This PCG algorithm will generate pseudo random number. The PCG is a variation of LCG – Linear Congruential Generator. The PCG algorithm is simple, fast, space-efficient and statistically good for generating random numbers. It is really very hard to

predict the random number generated by the PCG algorithm.

LCG applies modulo-2^n congruential generator. It is a linear function. Whereas PCG applies an output permutation function of LCG to improve the statistical properties of LCG. Permuted Congruential Generator algorithm consists of two parts. The first part is linear generator or recurrence. The second part is nothing but the permutation function. The permutation function of PCG is mainly used to ensure more randomness. This can be done by separating the state bits of the generator. The state bits are separated into pairs from the Cartesian products Z2 k × Z2 b−k. Then permutation is applied to 4 only one side of the pair.

Fig. 1 Some set of Frames in a GIF

The PCG algorithm also generate reproducible pseudo random numbers. This methodology is in need of reproducible pseudo random numbers since at the time of decryption, the same random frames has to be identified. The pseudo random numbers generated by an arbitrary seed to ensure reproducibility. This seed is used to generate a sequence of random numbers and while extracting the secret information, the same seed is used for finding the Stego-frames. Thus random sequence of frames can be selected with the help of PCG.

2.3 The Base64 Code for Embedding

Base64 coding is one way for encoding using HTML. It will convert different types of data to a series of letters and numbers. These converted data are HTML safe data. The different data types includes any type of image. With regard to the size in Base64 coding, 2K image is converted into 2.5K or 3K of Base64 data. Actually, Base64 is a group of similar binary to text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. Each Base64 digit represents exactly 6 bits of data. Therefore three 8-bit bytes can be represented by four 6-bit Base64 digit. A general approach is to choose 64 characters are both members of a subset common to most encodings. It is also printable.

The randomly selected frames are now converted into Base64 code. This code takes the size as specified above. This code is used for embedding the secret information. This code contains so much of information so that the secret information can be embedded into it. Hence the number of characters are more, it will be a very difficult task to distinguish the secret information and the Base64 code of the given frame.

The following figure named Fig. 2 depicts sample Base64 code for a frame, which is one among the frame selected in a random manner.

2.4 Vigenere Cipher Encryption and Embedding

The Vigenere cipher encryption method is a popular method for encryption and decryption. This Vigenere figure is formed with a 26×26 table with beginning to end as the line heading and section heading. The principal line of this Vigenere table has 26 English letters. Then in the beginning of the second line, each column has the letters moved to one side one position consistently. For instance, when the letter ‘B’ is moved to the primary position on the second line, the letter ‘A’ is moved to the end. This Vigenere table is used for encrypting the secret information. The traditional Vigenere cipher encryption method is used and the secret information is converted into cipher text. This cipher text is embedded into the randomly selected line into the randomly selected frame.

ISSN (Online) 2348 – 7968

www.ijiset.com

J4UeCkrG2494kdDUNTeLLTbS2qXd5cb4XLSpRlJJvZN4TeybexDc1FqzOK5xP4
8fKPOdle9qrVjaud/DvRT/AGpfB6bsbWy1q7vtSveZT0u0s51ry0lFpTjXpR3ptSaW
H97OY8y3IqtdYpo45nb3Tt747kc6+zw8cTmFzs+P9O1Gyo31jYXqhWi5Rjc0nQm
vLMZe8vPdeRDV2laiMxE/LH3lBPalvITEz18VI4w4P4S4/wBZ0viHjHhjTdV1DQ
5uppda5oKbsp8ylz0s/dlzQi+Zb+7HfZHHv627cq9ZG22OfL4Z6+kc27eqv1cVfNXv
FT9orhDwi0z7XxPxNWqXlTMLextJurXqzS6YW0VtvKTSWepD/m6qvPBXnHn
DH+VcnlXMz73GvCr9pLxG8XfEnVKUtV1DTuH1p8alpZRaTozUkm5VYPMpyz
LK5nFcqwk85+kejWgu2LVVzWx6zOOcbRPhGY+f2V7tzUXqeGLkxjz6n6uu1Lz
XfaOvV1i4rPLb9pcVHnL9W10/SPV00aWqOGLcRnwpj8KM06q1M3JuTPvqn87b
sn+pVpL37yrnKeHUbw1j/BFOlxO1P0WadZTMe1Viffnw66l8QuIJqcKqTTynnDT
MzZr5TBTqLU7xVDapa5qdCKjQ1u7pJfyXUo/k9yL/ABKJnM2on/6Y/Tb/ACYxt
cx/9X87/FlXHnHOnJOlr069FPK9pSpyT26SbjnGcdH8u4nszs65E8Vvhn3z9N/wjj
WdoUTEW7k1R7qf1+fjlIW/jHxbQcftmn6fWjFJteznCcvNZ5sJ9umPyKtzsLQTE8F
dUT8J/Efdct9qdpRMcdFMx8vzP2bOp+N2pK0lKy0KnRqKP/8AL7V5z6qKSx6M5
Gp9H9RX7Oju05/+aJj7TP59yxf7U1MUZpoiPdOfvEOVcRftAeIGl13qV7WqW1vh
wUKcotRf82ySbwtljr3PMXewO3tHdquauv8A8cRtVGJjOfClzy8Y5OVPaWqu17X
MT8uvrldOCf2g7itZU6mqa1Y6upxUsxpexrRT7z5Vj/6UcS52zqtFEzeoiqmOfdPzjb
6Qt2u2tRZ2vxE/SesOu8N8f8N8T0lKwvoRqN8rpzks83kvP4dfQ6+h7U03aFPFaq3
8Hb0vaVjVRmmcT114+SxnRdAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAHM/GHx44C8JtNcNc4jo0NSuZKjbWtGDr3NS
pJ4jGnRinKpNvZLGM9dlh8ntDtGnTxNqzObk/HHXg5mu7QpsRNFufa+3X9uLcI
8IV+L9VuPE7iThetw3qN/iP2nUqka2qSt47Qy9/Y5W/JnZvdZPL0zVRRFd6rEznO
fpOec/fwecoq46Yqqnfvzz7+s/Bb9KtuBPDLTLinwzotjp1GpN1rm5qSVL20+86k5b
y6vrtjphGl7tqucRRvMddckly/nM8+vz/bhfib+3pw5wvdz0PgjTLTXL6GY1LydZxsq
L8k+tVp7Plwv+bsYs3dVqI4qqeflnwj8x8fDOWkXrs05pphy/wD/ADr8W6rodS74n
nbzuXmEbSyU7alVbeElu38eaT7kdej1l7U+oq2+mO74zvt4q1caiu5NPF7O3XWGP
w/4Q1rxr1hcacbWVShaQ2jSrpNYy8KEe2M9+nfLPs/o36LWuydNF7XW4mud6aZ
jOPCqqJ7/AA74z3LNNcX59XZ2pjnPn5efjP8AT0FwfwZonBcs6G61JSTTTw8rrjO
Ez11/WVX4xVTG3v8A2W9FFr/Wurf3frK1O/lJ5cW36r5fEgi/VEYiIYns+3VOaqp
6+DHU1SFGPtK0VGOM5z1/X9DeL9U7YRz2ZR3VT111369PiKj7TE7WUo+k9
+vw+JtVdrxszT2ZRE71Zb9vxFozxzc1J5xmcc7+jWSvX62ecrFGlt0f60wkXe2NaL
hKtHEsbS2bz02ZWpqiv/WcpcTDQuLd0WmsuEkmn/TyN28Tlp1Lp063s5QeOVye
N9srH9TWqzNddNfdGUdWJuxHfGZ/CI1bgy94rt3a6baurF5l7zUYx+LezX1ZnUdt
6Ps+JjV3IiccuczN+fLfafNzdZpeKfYn3eU/jn1OJTOg+EHD+i29tNOcdaormc5b0Z
T32jF9sbLdZ2Pj/auqtazVXblijFFU7R18+Xwb0Wp4I453x1t9/FbqKpU7CtTr2dvTu
4L71Kny877Lz9Hk4vq6LNU+rp267o69yainhSmh8c6/pdX2cq0q1BNctKtNzjy+j6r
o1jovI6Gm7UvWZiJ3ie6Z/PP8eS9Y1t6xtE5jwlf9H4+0TUnGjdVFY15YXLWeINv
olLp9cM7ljtGzenhn2Z8/wBuxY7StXdq/Zn6fP8AazJprK6M6DoAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAKtxx4kcOcBUIT1edarc
VU/Y21BRdSpLGVFczSTeH1ZT1Ous6SqKbnOVPUa61p64t1c56673grxF/ad/ae8
a9fv+C+DeD73hHSKalTn9lr8qlGSwpVr3ClJYeeWjFdUpJ9Tez2H2129VVTZiLdq
NszOInbP+0ZmfdTGd8S8721l2pVFU0V1cMR/xjnPvnw+UPnR9f0b9n+9pcc+NlafE
XF93YwtdCp2dDPs6VKKjWq5l7kJNyhHmznlT5YrMk+P6Udg0+jddFNqv1k153i
MYx3bzPLbf4d0OdambketiiYzy8/xHx+bmviP+214j8SV523DdWjw/aJvlp2sVUrf+
utUT3/6YrfucHS9i3tb7V2eGJ38+/rfxykm1drzFU4927h+p8XcTcZXLueKdX1bWa
qfMlXr1K9Nf+mTaz28lhdMHWo9GdRVVFOjp45nwifptO3239zaaLdunOYz5+76J
HTuDOIOJq6gtN+yUZYlKpW91uPV4j6vB7b0f/wCnfaNd6i/q54KY5xPOfh8e/Cld
7Tsaanhpni9303/iXcfCn9nfT53FG/1Sx57eEnKnUq4bqPOW0u0X9fh3+m/4fZ3ZE
UxZoiq5TGImd5juzvyn3I9Na1XaU+svzMUT3csx+vv9XpnTdNs9Js6djYUI0qNJY
jGKwkc25cqu1TXXO70FFFNumKKIxENt1XTg8zUYp82X29cmmMy2aFxrC3hbt
z33fSK+X6RJTamebHFEPjTLDU+IbxUrWLqTWJTnLPJTWf4njzWdll7rcp9qdp6
TsWxN7U1YjljvmfKPHf8ALSa8RmeusLna8EaFYUoVNUuru+rRw3TjL2MM4/8
Ad+KPm+t/6hX70zTobcUx4zvP6+koouzPXX2SdCOl6c8abotG1nsvaJKUl574z59
zxnaHb/aOsnhu3apj37fKMI6p4ue79r6dZ31tcUZ393RncUpUp1FJc0eaOMrOd03tt
3RzNPeqtT62iqYmPDPd3536+utMxE8Sn/8AdfW9KpwjQvJahCnHepCXJz484t9X
6dz7b2Z6WaLW24jUTFFf4e+J5Ynw/S5TdpmcS37KyUv/EX0Zwz0pyWJP/qXVI
5fpH6XW+z6fUaGYruTHPnTT+Jny+ba9qaLdOKebdq6jb281H2zpyj0cFjHljY+QX
r969cqv3qs1zvMzz36+Dn13InfPXX3ZVxFTnKMK9zGqktpYxLv9ejLem11Uf7Rm
OvgxTemfOElbVKV08U6i6Nv0wu6Opbv27sZplNTVFUZh+V404Jquo7b7tdt85/q
bVcM82WnK5TlJKUatJv+FqW2ye2/fP4dSKqmqnExPXv/AH4T8deLfCS0bxEu+A
eWvfTrXuhuUYyo82Z0MtLmp5fT/lzh+j3fS0XalVifV3czH1jrw+Xe6Ok1tdmqInen
7e79Oz6Fr+j8S6dDVtCv6V5aVNo1Kb79011TWej3PTW7lF2mK6JzEvQW7tF6ni
onMJA3SAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA2opy
k0kllt9gcnMvFXxn0Xw94av+Ir66Vvp9nDDr9alao/u06UXs23sm/XbHvHF1nasW4
n1Xz8Z8I/e8eW+XC1vakxmjT/P9fv8At4D1j9pDWv2gOKIaBU4Zs4WHvxlCjcVvt
FOE9p1HcPEZPde7ye849e6djdg6ztnXUUU0ZxMTVVO8UxnnPvxMRHOeXdMx
wb9+jSf+Wucz9c9Zdw4G4V07gzh200PS611WhTipSq3NRznOTSy3np0WySWx9
uiijS2/U2uUdTuq2bc37kXbvljb3Yz/AD91B/aL8LdT8SNJ0i+0y5UKujyuITSg51H
TqqH3d87OEfM4HaXo5pu371qnU3JoiiZnaI3ztMb7RyjnE+GO9e1F65RZ4rVPFP
8AGfj17nF9E/ZwvKM41I6LXuqnM2p3D5cdPdxLGM47eR6fRdidi9lxE0xFU+NX
tT7/AC+GI8HCqudpanlTMe7b77ulaF4Caq5wVShaW0EsL3G316rGP4fXv3OjV2p

Fig. 2 Sample Base64 code of a frame

2.5 Embedding Cipher Text

After the secret information is converted into cipher text using Vigenere cipher method, the same has to be embedded into the Base64 code of the randomly selected frame. In the Base64 code also the lines numbers are selected in a random manner. Here another seed is used and the sequence of random numbers are generated. In this point, these random numbers are treated as line numbers in the Base64 code and in those line numbers of the frames, the secret information is encrypted and embedded. Instead of embedding the original secret information, it is converted as cipher text using Vigenere cipher method and then it was embedded. First a set of frames are selected based on the sequence of random numbers generated using PCG and a seed. Then set of line numbers are selected randomly with the help of PCG and another seed. In these lines of those selected frames, the cipher text is embedded.

Then the embedded Base64 code is again converted into a frame. After all these frames are generated from the corresponding Base64 code, these frames are converted back to a GIF image. This is the Stego-image which holds the entire encrypted secret text. The Fig. 3 shows a randomly selected one original frame and Fig. 4 shows the corresponding Stego-frame. This will show the visual effect of the original frame and Stego-frame. This is given for visual comparison.

Fig. 3 Original Frame

Fig. 4 Stego-Frame

3. The Extracting Methodology

In this section, the extraction of the original secret information from the Stego-image is explained. Here the Stego-GIF image is taken as an input then it is converted into frames. The same number of frames are generated. As mentioned above, for the given GIF, 124 frames are generated. Then by using the same first seed, sequence of random numbers are generated with the help of PCG pseudo random number generator. These random numbers denotes the specific Stego-frames which contain the secret information. Then with the help of the second seed and PCG, the second set of random numbers are generated and these depicts the lines numbers of the Base64 code of the corresponding frames where the secret information is available. Hence the secret information can be extracted.

Now the secret information is available as a cipher text and Vigenere cipher table is used to encode the cipher text. Finally the original secret information is extracted from the GIF image.

4. Review of Related Work

Enormous researchers have presented their various approaches in the field of Steganography and cryptography. The following gives the brief review of some recent researches.

Kousik Dasgupta et al. proposed Genetic Algorithm based optimized video Steganographic approach. In that they optimize the values over basic vide steganography using 3-3-2 LSB technique. They used cost function in the optimizer. That cost function consists of two factors. In their work, the PSNR values lies between 20dB and 40dB. They applied this technique in an uncompressed domain.

Shivani and Paramjeet developed video steganography with digital watermarking techniques. They combined Steganography and watermarking for the protection of the secret information. They also used Least Significant Bit insertion for embedding the secret information. Then by using the Discrete Wavelet Transform, they divide the image signal into high and low frequency parts and they used the high frequency part for watermarking. They also used Discrete Cosine Transformation for watermarking the digital image.

Navdeep and Neha introduced an algorithm of steganography, which hide a text file inside an image. They maximized the storage capacity by using an algorithm for compression. This algorithm compressed the data, which is to be embedded. This particular algorithm used by them worked in a range of 1bit to 8 bits per pixel ratio. Thus by applying this algorithm they developed an application that supports efficient way to hide data.

Sudeepa et al. developed a methodology for video steganography. In that method they used randomization of frames. They used Feedback Shift Register (FSR) method to generate pseudo random numbers. Their algorithm contains two phases. The first phase select random frames using FSR and in the second phase, the secret information to hided is encrypted by performing XOR operation with the selected secret key. They parallelized their entire operation with the help of the threads. They also used Least Significant Bit insertion for embedding the encrypted secret information.

Shikha and Vidhu proposed a method to hide the secret text in image with the help of Matlab. They divided their work totally into four parts. The first part is used to encrypt the text. They encrypted the text using play fair method. The second part is dedicated to encode the encrypted text in to the image file by using the Matlab code. The third part is devoted to decode the image file, and to extract the encrypted text message. For this also they used Matlab code. Finally the fourth part is for decrypting the cipher text message using play fair method.

Aryfandy et al. published a survey of steganographical methods in the different files like text, audio, image and video. In text steganography, they discussed about the three methods named Format based method, Linguistic method and about the final method named Random and Statistical generation method. They also discussed about Selective hiding, Semantic hiding and Hiding Using Whitespaces in the same. Then in image steganography they discussed about Spatial Domain Technique with the Least Significant Bit, Transformation Domain Technique, Distortion Technique and Masking and Filtering Technique. In audio steganography, they specified about the three different techniques called LSB Coding, Parity Coding and Echo Data Hiding.

Xinyu et al. presented a visual steganography technique which will hide a full-sized color image or video file within another image or video. They used neural network for video steganography. They developed a temporal residual modeling technique to completely utilize the sparse property of inter-frame differences. They also developed a separately treating reference and residual frames during the generation of Stego-videos.

MrudulDixit et al. embedded secret information in a cover video. They also used Least Significant Bit replacement algorithm. They embed the secret data by replacing the LSB of the pixels in the carrier video frame. Then they checked the quality of Stego-video with the help of different parameters like computing the difference between mean of the cover frame and the Stego-frame, PSNR and RMSE.
Shahd specified another method for video steganography. In that she first isolate the audio from the video file then convert every colored frame into binary value of 24 bit each and represent the secret text file in 16 bit length in a secret location. Finally she used Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) to measure the performance of her work.

Yunxia Liu et al. manipulated embedded position of secret message. To manipulate this position, they divide video

steganography into three categories named intra-embedding, pre-embedding and post-embedding. Intra-embedding methods further categorized into intra-prediction, motion vectors, pixels interpolation, transform coefficients. They used Pre-embedding method to manipulate on the raw-video and the Post-embedding to focus on the bit streams. They concluded with the performance assessment by H.265 video steganography and reversible video steganography.

Rajalakshmi and Mahesh proposed a technique to mask the existence of the message. They dealt with video steganography algorithms to hide one video file within another video file. For the implementation of this method, they used Patch wise Code Formation techniques. This technique provides a better video quality and also the authentication ability. Then finally they measured the performance of the process with the help of PSNR, MSE, CR and BPP.

Sagar and Vinit analyzed various steganographical methods. They tried steganography with the help of Binary file technique, text technique, Least Significant Bit, DCT and Wavelet transformation. In their work they provide, along with encryption of the secret Digital media the secret data with authentication security. This provides double protection for the secret data.

Yuting Su et al., developed a steganalytic approach. This approach is motion-vector-based approach of steganography for video sequences. They used a SVM classifier. That classifier is based upon twelve extracted features in spatial and temporal domain. This classifier is used to detect the Steganographic data.

Nithya Kalyani and Mahesh used Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) for hiding secret data. They chose video file as cover medium. Finally they computed the Peak Signal to Noise Ratio to compare with the original frame.

5. Conclusions

The methodology proposed in this paper is effective because it is an application of both Steganography and Cryptography. The reason for selecting GIF is the ease of frame conversion method. After converting GIF into frames, two different seeds are used to generate two set of pseudo random numbers. These sequence of numbers used to select random frames and random line numbers in the selected frames. Thus this technique supports complete randomization. Anyone cannot predict which frame is used to embed the secret information and which line in the frame contains that secret information. The Base64 code contains only characters of the equivalent image. If the secret information is embedded, all together contains the set of characters. Hence embedding can be effective. Also the secret information is not directly embedded, instead it encrypted and embedded. This add more security to the secret information. After converting the Base64 code to Stego-frame, visually there is no difference between the original frame and the Stego-frame and hence the original video and the Stego-video is same.

References

[1] B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 2002.
[2] Kousik Dasgupta et al., "Optimized Video Steganography using Genetic Algorithm (GA)", in International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA), 2013, Vol. 10, pp. 131-137.
[3] Shivani Khosla and Paramjeet Kaur, "Secure Data Hiding Technique Using Video Steganography and Watermarking", International Journal of Computer Applications, Vol. 95, No. 20, 2014, pp. 007-012.
[4] Navdeep and Neha Goyal, "Hide Text in Images Using Steganography and a Review of Methods and Approach for Secure Steganography", International Journal of Research in IT & Management, Vol. 6, 2016, pp. 064-073.
[5] Sudeepa K B et al., "A New Approach for Video Steganography Based on Randomization and Parallelization", in International Conference on Information Security and Privacy (ICISP), 2016, pp. 483-490.
[6] Shikha and Vidhu Kiran Dutt, "Steganography: The Art of Hiding Text in Image using Matlab", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, 2014, pp. 822-828.
[7] Aryfandy Febryan et al., "Steganography Methods on Text, Audio, Image and Video: A Survey", International Journal of Applied Engineering Research, Vol. 12, No. 21, 2017, pp. 10485-10490.
[8] Xinyu Weng et al., "Convolutional Video Steganography with Temporal Residual Modeling", Semantic Scholar, 2018.
[9] MrudulDixit et al., "Video Steganography", in International Conference on Pervasive Computing, 2015, pp. 001-004
[10] Shahd Abdul-Rhman Hasso, "Steganography in Video Files", International Journal of Computer Science Issues, Vol. 13, No. 1, 2016, pp. 032-035.
[11] Yunxia Liu et al., "Video steganography: A review", Elsevier-Neurocomputing, Original Software Publications, 2018.
[12] K. Rajalakshmi and Dr. K. Mahesh, "Video Steganography based on Embedding the Video using PCF Technique", in International Conference on Information, Communication & Embedded Systems (ICICES), 2017.
[13] Sagar S.Pawar and Vinit Kakde, "Review on Steganography for Hiding Data", International Journal of Computer Science and Mobile Computing, Vol. 3, 2014, pp. 225-229.

[14] Yuting Su et al., "A Video Steganalytic Algorithm Against Motion-Vector-Based Steganography", Elsevier-Signal Processing, Vol. 91, 2011, pp. 1901-1909.
[15] D. Nithya Kalyani and Dr. K. Mahesh, "Safe Information Hiding Using Video Steganography", International Journal of Computer Science and Mobile Computing, Vol. 4, No. 7, 2015, pp. 502-512.

Dr. Vani Perumal received M.C.A degree from the Department of Computer Applications, Bharathidasan University, M.Phil and Ph.D degree from the Department of Computer Science, Mother Teresa Women's University. She is currently working with the IT Department in Rustaq College, Ministry of Higher Education, Sultanate of Oman. Her research interest includes Steganography, Data mining, Machine learning, Pattern recognition, Biometric Image processing, Data Compression and Nano Technology.