ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

A NOVAL APPROACH IN REVERSIBLE DATA HIDING FOR STEGANOGRAPHY

*Dr. P.Marikkannu M.Tech,Ph.D
**Anjana C

*Assistant Professor, Department of IT, Anna University Regional Campus, Coimbatore.
**PG Scholar, Mobile and Pervasive Computing, Anna University Regional Campus, Coimbatore.

Abstract: Data security is becoming important with the bulk increase of digital communication in the internet. There is no use or meaning of doing communication using extremely high end technologies if there is no privacy. Many encryption techniques are used to protect data but Steganography is a singular method of data hiding inside some carrier. This paper focus on utilization of digital video as a cover to hide data and ensuring more security using steganography. In the proposed method the secret data is embedded in the video after framing it. Patching of each frame and embedding secret data gives higher level of security and resistance against extraction by attacker. Embedding capacity of secret data which is proportional to the size of Stego frame. Reversible capability of the proposed method provides functionality which allows recovery of source frame. The proposed algorithm can provide high embedding capacity comparing to the prevailed approaches.

Keywords: Cover Video, Steganography, Stego frames, PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), Data embedding.

1. INTRODUCTION

In the field of Data Communication top priority is given to Steganography. Now a days the use of computers become part of human life. So securing data is becoming a highest issue. The concept of hidden transfer of information is concerned here. Cryptography and steganography are well known and widely used techniques that manipulate information in order to hide their existence.

Steganography is the science of hiding messages in a medium called carrier or cover in such a way that existence of the message is concealed. Host medium used in Steganography generally includes meaningful digital media such as digital text, image, audio, video and 3D model etc. Cryptography is the other way to hide secret data over the network, by converting plain text into cipher text. Cryptography provides Privacy, Confidentiality, key exchange and authentication but explore the fact that communication is happening. Steganography takes cryptography a step farther by hiding the existence of secret data. There are many types of algorithms in cryptography and Steganography, thus it is very difficult to identify by the attackers which algorithm is supposed to be used. Steganography and Cryptography both are data security techniques. Steganography can use in Cryptography whereas Cryptography cannot be used in Steganography. If we implement Steganography over Cryptographic data which will increase the security level.

It requires a cryptographic decoding key to extract the hidden message in the receiver side. The requirement of any data embedding scheme can be categorize into security, capacity and robustness. The objective of this paper is to improve the capacity of the data to be hidden inside the carrier video. The proposed scheme is a data embedding method that uses high resolution digital video as a carrier. The proposed scheme provides to embed a significant quantity of information making it different from typical data embedding method.

Data embedding requirements include the following:

1) Imperceptibility: The video with embedded data and original data source should be perceptually identical.

2) Robustness: The embedded data should survive any operation the host signal goes through and preserve its fidelity.

3) Capacity: Maximize the data embedding payload inside the carrier.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

4) Security: Security is in the key for embedding the data.

The remainder of this paper is organized as follows: In section II, review the patch synthesis technique. In section III, defines methodology of proposed work. In section IV, cover the parameters. In section V, consist of results and discussions. In section VI, describes conclusion.

2. RELATED WORKS

The secret data communication techniques were performed during ancient times using chemicals, mediators etc. The secret data is hidden in the mediator's body or on the mediator's body as similar approach for Reversible Data Hiding. As cover frames in image steganography, gray scale, binary or color images may be used for hiding the secret data. It is a science handling with the hiding of the secured information in a harmless signal.

In most image data hiding methods, the single host image used are distorted due to embedded data. This leads to two drawbacks. First, since the size of the cover image is constant, the more secret messages which are embedded allow for more image distortion. Also embedding capacity will be directly proportional to the size of cover image. The main objective of this work is to hide the secret message in a high resolution video. This will overcome the capacity as well as the distortion problem.

Roshan Bonde and Parag Jawarkar in Reversible Data Hiding Through Histogram Shifting [1] With A General Framework (2015), describes a novel method of Stegnography to achieve Reversible Data Hiding (RDH) is proposed using Histogram Modification (HM). For this a single image is used.

For the texture synthesis analysis, Anton Alstes Wang Tiles [2] For Image And Texture Generation (2014) , discusses the use of Wang Tiles for image and texture generation, creating large area of non-periodic texture, point distributions or geometry can be efficiently done at run time by constructing a tiling of the plane using a few set of Wang tiles. Wang Tiles are squares whose edges are each assigned a color. The method consists of filling a tiny set of Wang Tiles with texture, Poisson point distributions or geometry and non-periodically tiling the plane to stochastically make a continuous representation. This is complex and difficult to result a fast output.

Infant Jini and Priya.S.V [3] in Reversible Data Hiding Using Line Based Cubism Image (2014) details the data hiding as a technique for watermarking and other such applications, which imprints data imperceptibly in to a cover image so that people cannot see the existence of the hidden information in the resulting stego-image (or stego-media). The method finds line segments in the source image by the Canny edge detection method and the Hough transform, combines nearby line segments, widens the remaining lines to the image boundaries, and re-color the created regions by their average colors, to make an abstract type of the real source image as the desired art image. Use of binary image and then to recolor them resulted more computational timing.

Otori and Kuriyama [4], [5] pioneered the work of combining data coding along with pixel-based texture synthesis. Secret messages to be hided and are encoded into colored dotted patterns and they are directly painted on a plain image. A pixel-based algorithm coats the rest of the pixels using the pixel-based texture synthesis technique thus consisting the existence of dotted patterns. To extract messages the printout of the stego synthesized texture image is taken before applying the data-detecting mechanism. The capacity provided by the method of Otori and Kuriyama is based on the number of the dotted patterns. However, their method had a small error rate of the message extraction.

Ravneet Kaur and Tanupreet Singh in Hiding Data in Video Sequences using LSB with Elliptic Curve Cryptography [6] with a general framework (2015), describes about the advantages of encrypting the key used in the embedding process. The main aim of this paper is to make the key is very confidential by using ECC(Elliptical Curve Cryptography). As ECC provides better security with smaller key sizes, results in faster computation, Lower power consumption along with memory and bandwidth saving. From the past results, it is identified that Steganography when compared with Cryptography provides better results.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde pioneered the work of Advanced Video Steganography Algorithm [7] (2013) describes a new Steganography algorithm such that the LSB and the LSB+3 of the cover file in alternate bytes. The last 300 bytes of the cover file is used for the creation of password. Retrieving of secret message bytes by bytes and convert it into corresponding bytes.. DCT and DWT transformations are mainly used in this paper. This paper is also demonstrate for Bit exchanging and Indexing method.

3. PROPOSED WORK

The model of proposed algorithm uses cover video as a carrier for secret data transmission. Here the carrier file (AVI file) length is collected and checked if it is eight times bigger than that of the text file. Detect the starting point of the data in the AVI file and create the secret key by imprinting the content totally to the AVI file. The carrier file is split into frames of equal size. Each frame is then put under patching process which is similar to that of image steganography. The output obtained for this system is a stego'd video file. The stego video is send via communication channel. At the receiver side, the same stego video is received. The secret data and the secret key can be extracted by using appropriate extraction methods.

3.1) BASIC MODEL

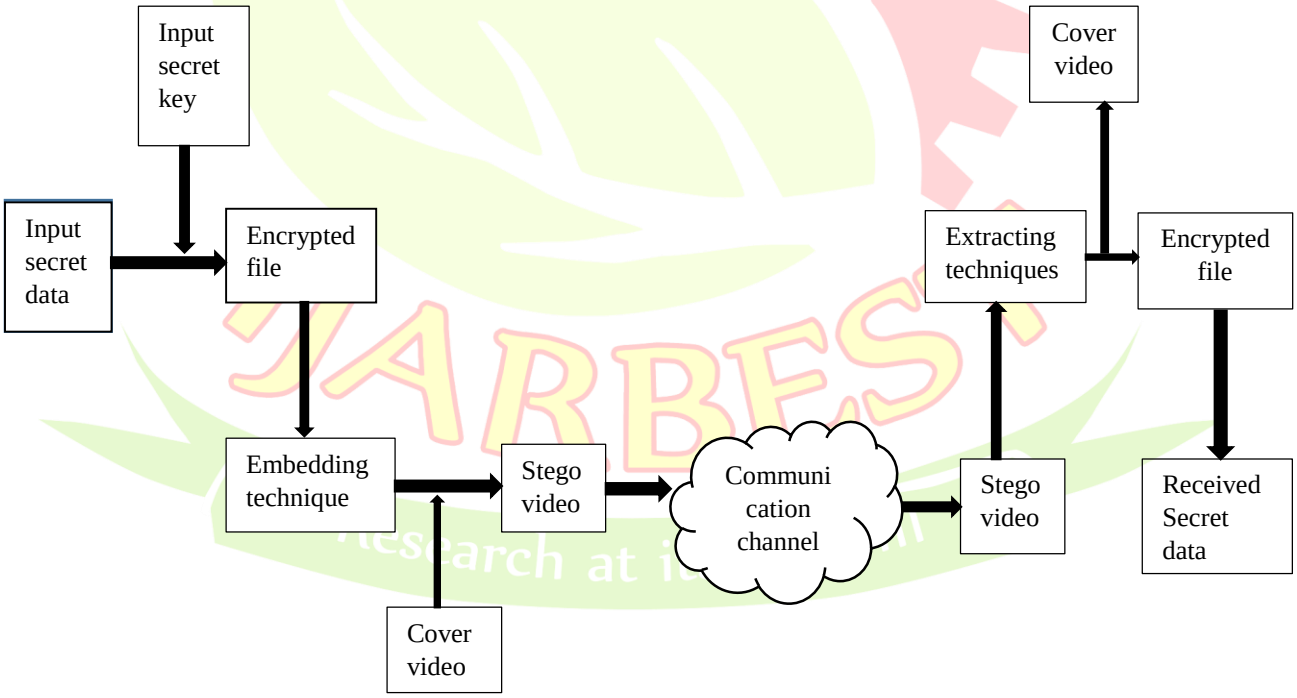


Figure 1:Basic Model

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Frame synthesis is a method of computationally creating synthetic frames. It is important for applications in computer graphics, computer vision and image processing. Frame synthesis is the creation and placement of frames through computation and procedural generation. Each frames are taken individually and split into patches which is the basic unit used for steganographic frame synthesis. The patch which is used for synthesis is shown in Figure 2. The secret data will be hidden in each patches.

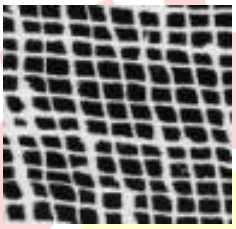
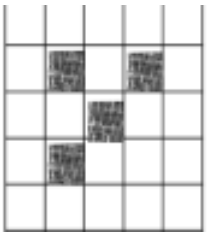


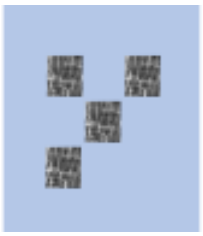
Figure 2: Texture image

Figure 3: Synthesized texture after weaving

A patch represents an image block of a source frame where its size is user-specified. The size of a patch by its width (Pw) and height (Ph). A patch contains the central part and an outer part where the central part is referred to as the kernel region with size of Kw×Kh, and the part surrounding the kernel region is referred to as the boundary region with the depth (Pd). Next, here describe the concept of the kernel block. Given a source video and frame it with equal size. Each source frame will contain number of patches with the size of Sw×Sh, which can again subdivide the source patches into a number of non-overlapped kernel blocks, each of which has the size of Kw×Kh. Let KB represent the collection of all kernel blocks thus created, and ||KB|| represent the number of elements in this set. The indexing for each source patch kbi, i.e., KB={kbi| i = 0 to ||KB||-1}. As an example, given a source patch with the size of Sw×Sh = 256 × 256, if set the size Kw×Kh as 64 × 64, then can generate ||KB|| = 16 kernel blocks. Each element in KB can be identified as {kb0, kb1, …, kb15}. Then expand a kernel block with the depth Pd at each side to produce a source patch. The expanding process will overlap its near by block. If a kernel block is located around the boundary of a source frame, operate the boundary mirroring using the kernel block's symmetric contents to produce the boundary region, for the kernel block kb4. Similar to the kernel block, can denote SP as the collection of all source patches and SPn=||SP|| as the number of elements in the set SP. It can employ the indexing for each source patch spi, i.e., SP={spi| i = 0 to ||SP||-1}.

The steganographic patch synthesis algorithm needs to generate candidate patches when synthesizing synthetic frames. The concept of a candidate patch is trivial: employ a window Pw×Ph and then travel the source texture (Sw×Sh) by shifting a pixel each time maintaining the scan-line order. Let CP={cpi|i=0, 1, …, CPn-1} represent the set of the candidate patches where CPn=||CP|| denotes the number of elements in CP. When generating a candidate patch, need to ensure that each candidate patch is unique; otherwise, may extract an incorrect secret message. In the implementation, here employ a flag mechanism. First, check whether the original source texture has any





ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Figure 4: Index table and Composition image placed with source patches

duplicate candidate patches. For such a patch, set the flag on for the first one. For the rest of the duplicate candidate patches set the flag off to ensure the uniqueness of the candidate patch in the candidate list.

There are three main process in the transmitter side. They are index table generation, patch composition process and message oriented patch synthesis. The first process is the index table generation is to produce an index table to note the location of the source patch set SP in the synthetic frame. The index table allows the source frame completely. Such a reversible embedding style open out one of the major benefits proposed algorithm offers. Here first determine the dimensions of the index table (Tpw×Tph). Given the parameters Tw and Th, which are the width and the height of the synthetic frame intend to synthesize the number of entries in this index table can be determined using equation 3.1, where TPn denotes the number of patches in the stego synthetic frame. For simplicity, chose appropriate parameters for Tw, Th, Pw, Ph, and Pd, so that the number of entries is an integer. .

$$TPn = TPw \times TPh = \left[\frac{(Tw-Tp)}{(Pw-Pd)} + 1\right] \times \left[\frac{(Th-Tp)}{(Ph-Pd)} + 1\right] \quad (3.1)$$

The source patches can distributed in a rather sparse manner if the synthetic frame has a resolution that is much larger than that of the source frame or the source patches may distributed in a rather dense manner if the synthetic frame has a resolution that is slightly larger than that of the source frame. For the patch distribution, avoid positioning a source frame patch on the borders of the synthetic frame. This will encourage the generation of borders by message-oriented frame synthesis, enhancing the image quality of the synthetic frame. The index table has the primary values of -1 for each entry, which shows that the table is blank. Now, need to re-assign values when distribute the source patch ID in the synthetic frame. In the implementation, employ a random seed for patch ID distribution, which increases the security of the steganographic algorithm making it more difficult for malicious attackers to extract the source frame. As a result, the index table will be scattered with different values as shown in Figure 4 where four source patches.

In the above index table, the entries with non-negative values indicate the corresponding source patch ID subdivided in the source frame, while these entries with the value of -1 represent that the patch positions will be synthesized by referring to the hidden message in the message-oriented frame synthesis. Considering the above condition, now use the surf location with strongest points to disarrange the ID of the source patches subdivided in the source frame. The second process is to paste the source patches into a workbench to produce a composition frame. First, establish a blank frame as workbench where the size of the workbench is equal to the synthetic frame. By referring to the source patch IDs stored in the index table, paste the source patches into the workbench. During the pasting process, if no overlapping of the source patches encounter, paste the source patches directly into the workbench.

Embed the secret message via the message-oriented frame synthesis to produce the final stego synthetic frame. Secret messages will be encoded in the remaining blank locations during the message-oriented frame synthesis. Secret data will be hide inside the selected patches. In order to read the secret data first it needs to convert it into binary format and then embed the secret data in the identified location. Hence, generate the Stego frame. Message extraction is the process of extracting the message from the stego frame at the receiver side. Using a secret password (between sender & receiver), the receiver can extract the message from the stego video. This password helps the receiver-side to recreate the same sequence used in the sender-side. This helps to retrieve the secret message as well as the stego synthetic frame.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

3.3) FLOWCHART

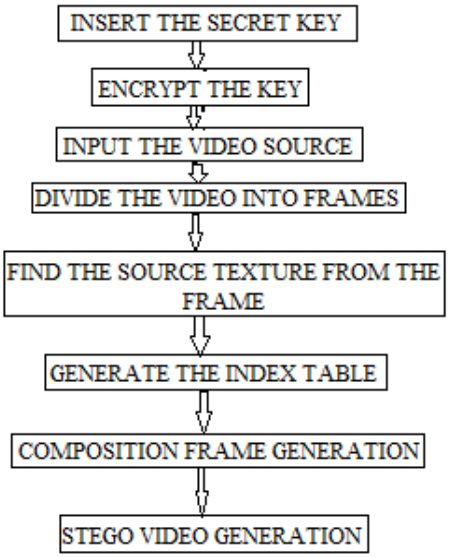


Figure 5: Flowchart of Transmitter Part of Proposed Algorithm

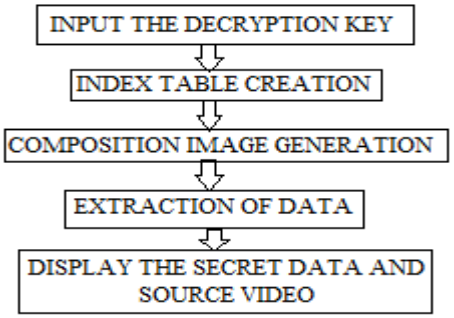


Figure 6: Flowchart of Receiver Part of Proposed Algorithm

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Working: Initially a secret key is defined, called an Encryption key. The encryption key must be remind by the user to undergo successful decryption. Once the encryption key is entered it will be stable till the process completes. Next the video for hiding secret data have to select. For this a high resolution AVI video is chosen. After that the selected video is framed into equal sizes. In each frame the strong points is found. These strong points gives the source patches or source patch location. A composition frame is then generated where the text embedding frame is placed. The secret message is embedded with this composition image. The source patches are fused with the composition frame. Now the frame generated is mostly similar to the source frame. This fails the attack of steganalytic attackers.

In the receiving end initially, the decryption key is to be entered. This shows the security of the system. As well the data and video is retrieved without any error to implicit the reversibility nature of the proposed algorithm. All these factors was initially faced as threatening to the data hiding field. The embedding capacity is also another problem. Here compared to the existing techniques the data hiding capacity is very much improved.

3.2 PARAMETERS USED

This section demonstrates the performance of the proposed method.

The parameters used in this paper are:

PSNR: The quality of image/video of each steganography method is expressed in PSNR(Peak Signal to Noise Ratio). PSNR measure the quality of the video by comparing original video with the stego video. Higher the PSNR, the better the quality of the compressed or reconstructed image. The PSNR values can be obtained using the following formula:

$$\text{PSNR}=10\log_{10}\left(\frac{MAX^2}{MSE}\right)$$

MSE: Mean Square Error is the measure used to quantify the alteration between the original and the distorted video. MSE is calculated by using the following formula.

$$\text{MSE}=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y)-S(x,y))^2$$

4. RESULTS AND EVALUATIONS

The proposed system was implemented on MATLAB platform. High resolution video frames can carry more secret information. Here in this paper consist of 6 frames. Each frame is further divided into patches. Embed the secret information as well as the secret key in those patches along with the source patches. This lead to the formation of Stego frame. After the process of embedding on the selected patches there was no human eye perceptible difference in the resulting frame. The correct decryption key is given in the receiver side provides the original video and the source patches.

In this paper, the experiments are done with a short length video clip. Each frame is executed with a predefined time. Finally the Secret data is received at the receiver side along with the Peak Signal to Noise Ratio (PSNR) as well as Mean Square Error (MSE) gives a good idea about the prevailed approaches and the proposed method.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Figure 7: Video Frames

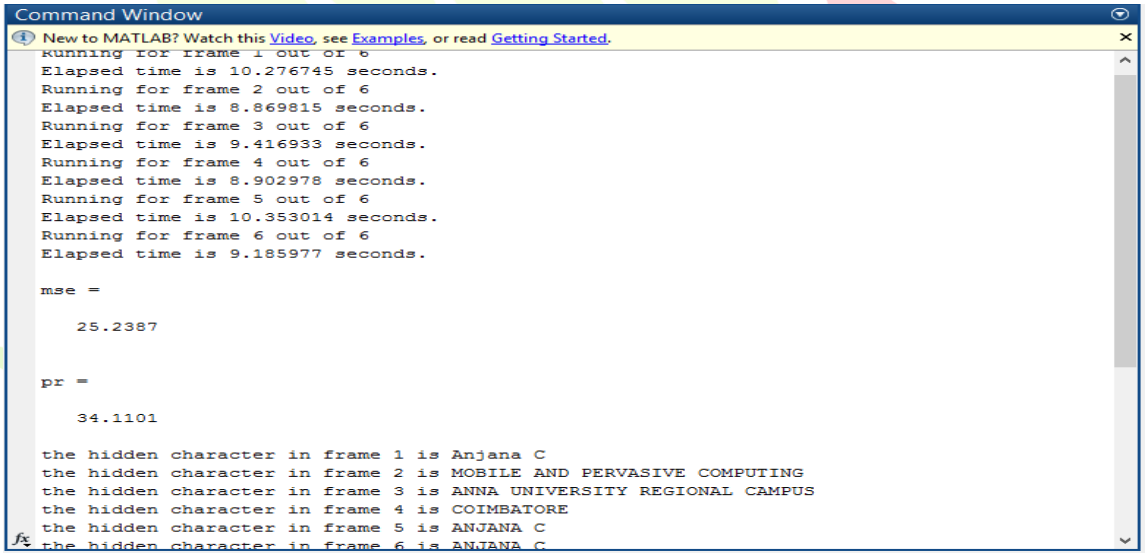


Figure 8: PSNR and MSE calculation along with Secret data.

5. CONCLUSION

The proposed System is based on the research findings which would be able to hide data into video frames (AVI) that provides a robust and secure way of data transmission. Steganography is an effective way to obscure data and hide confidential information. The result of Steganography is amplified by combining it with cryptography.

In future the cover image is protected with personal passwords so it is not possible to damage the data by unauthorized person also increase in number the frames results more data embedding capacity. Hence this paper focuses on increasing Security, increasing PSNR and reducing Distortion rate.

6. REFERENCES

[1] Roshan Bonde and Parag Jawarkar, (2015) "Data Hiding through Histogram Shifting", International Journal of Electrical, Electronics and Data Communication (IJEEDC) , vol.3, No.7.

[2] Anton Alstes, (2014), 'Wang Tiles for Image and Texture Generation', Seminar on Computer Graphics Springer, Vol. 18, No. 5, pp.789-795.

[3] Infant Jini N.S and Priya.S.V, (2014), 'Reversible Data Hiding Using Line Based Cubism Image', IJREAT International Journal of Research in Engineering & Advanced Technology, Vol.2, No.2, pp.121-125.

[4] Hirofumi Otori and Shigeru Kuriyama,(2014), 'Texture Synthesis for Mobile Data Communications', IEEE Computer graphics and applications, Vol.2, No.20, pp.1011-1016

[5] Kuo-Chen Wu and Chung-Ming Wang, (2014), "Steganography using reversible texture synthesis", IEEE Transaction on Image processing., vol.10, No.19, pp.121-125.

[6] Anders Hast and Martin Ericsson, (2010), 'Multiscale Texture Synthesis and Colourization of Greyscale Textures', WSCG Communication Papers, Vol.25, No.19, pp.12-14.

[7] Pritish Bhautmage*, Prof. Amutha Jeyakumar**, Ashish Dahatonde "Advanced Video Steganography Algorithm" Vol. 3, Issue 1, January -February 2013, pp.1641-1644.

[8] Bi.H.T.Wu and J.Huang, (2012) 'Reversible image watermarking on prediction errors by efficient histogram modification', Signal Process, Vol.92, No.12, pp. 300–309.

[9] Poonam V Bodhak, Baisa L Gunjal "Improved Protection In Video Steganography Using DCT and LSB", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[10] Abhishek Mangudkar, Prachi Kshirsagar, Vidya Kawatikwar, Umesh Jadhav "Data Hiding Technique using Steganography and Dynamic Video Generation" , International Journal of Scie

[11] J. Dittmann, M. Steinebach, I. Rimac, S. Fischer, and R. Steinmetz "Combined video and audio watermarking: Embedding content information in multimedia data. In Security and Watermarking of Multimedia Contents", pages 455–464, 2000.

[12] Kedar Nath Choudry, Aakash Wanjari "A Survey Paper on Video Steganography" International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2335-2338.

[13] Manpreet Kaur, Er. Amandeep Kaur "Improved Security Mechanisam of text in Video by using Steganographic Technique: A Review",International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 5, May 2014.

[14] Jessica Fridrich and Miroslav Goljan, (2014), 'Reliable Detection of LSB Steganography in Color and Grayscale Images', IJREAT International Journal of Research in Engineering & Advanced Technology, Vol.12, No.3, pp.234-238.

[15] Zenon Hrytskiv, Sviatoslav Voloshynovskiy and Yuriy Rytsar (2013), "Cryptography and Steganography of video information in modern communications", International Journal of Electronics and Energetics vol. 11, No.1, 115-125.

[16] Prof. D P Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak "Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithms in Video Steganography" International Journal of Engineering Research and Applications (IJERA)Vol. 1, Issue 2, pp.102-10.