International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

An Approach to Identify Weaker-to-Stronger Image File Format To Build A Robust Image Steaganography

Sreekanth Nara[1] , Dr. M.H.M.Krishna Prasad[2]

[1]*Research Scholar at Rayalaseema University, Kurnool (D), AP, (India)*

[2]*Professor & Head, CSE Dept, JNTUK, Vizayanagaram, AP,(India)*

ABSTRACT

Over a decade Image –Steaganography technique is treated to be the safe way to transfer secret information. But the misuses of this concept lead to identifying the weakness of this method to safeguard the intellectual property. In this paper, we would set up an experiment using video editing software tool. Through which one can generate many images of same image type in a specified folder. Since we have different kinds of image formats like BMP, PNG, JPEG, TIF, DPX, and EXR to judge the complexity of Image Steaganography with particular image format. We need to check each image file type, we repeat the experiment setup for all the image formats and gather the data of the same kind in a specified folder. After collecting the data, we try to do some statistical analysis with and without hidden data with each type of image. By creating column charts for the same, one can guess if there is any hidden information in any image file or can suggest which image file format is / not suitable for Image Steaganography.

General Terms:Image –Steganography, Render As, Image file formats

Keywords*:*Video Standards, Resolution, Image- Steganography

1. INTRODUCTION

Image Steganography is the art and science of communicating secret information, by hiding information in a picture, which takes a good amount of time for the cracker to break the code. Most of the related work in the Image Steganography focus on Jpeg and BMP type of image files. In recent years, the research in Image Steganography has extended to other kinds of image file types. Especially resolution and file size of original TIFF, PNG image files properties are unique, when compared to the same kind of image data of any other standard resolution opted. A detailed review of the list of image file formats like BMP, DPX, PNG, JPEG, WMPHOTO, EXR and TIFF, information can be obtained through the experimental setup.

1.1 RELATED WORK

Souvik Bhattacharyya et.al.,[17,21,22,23] has studied about Image Steganography, which reveals the flexible implementation using jpeg image file, audio, video formats. But suffers from limitation like different algorithms

have to be developed, or slight changes had to in the existing algorithm based on the type of Image file format used, here jpeg image file format is selected and to strengthen it different techniques or algorithms have been used. Fridrich, J et.al., [4] introduced a new approach for implementing image Steganography through the dithering algorithm on jpeg image file. Over a past decade, this was the hot topic about the security trends in information technology. Sreekanth Nara et.al., [1] has discussed the detailed process for breaking the image Steganography using jpeg image file type to get the hidden information. Farid. H et.al.,[3] proposal suffers from a counter attack. Hany Farid [2] approach is better for image Steganography for jpeg image file format. Similarly, Armin Bahramshahry et.al.,[13] tries to strengthen it by encrypting the secret information before embedding into the picture. But a good cryptanalyst can break the code. Now it's the time to find an optimistic image file format to make easy thing more tough for practical use of Image Steganography for the right cause and easy to detect if there is any misuse, provided one has good knowledge about the properties of a picture on various types of Images. Abhishek Mangudkar et.al.,[12] approach to transfer secret information is right, but it also has limitations, which will be elaborate in detail, Our proposal requires a stakeholder like Statistical Data Analyzer, Video Editor, and Image format analyzer.

1.2 PROPOSED SYSTEM ARCHITECTURE

In the figure 1.2, Which represents the system architecture for implementation of Video Steganography. Which would help us to find weaker to stronger Image File Format at a fly, by spending little time over generating various images of same type with same resolution. Were it would be used to analysis and resolve the ambiguous Image File format, if used for implementing Image Steganography. The explanation of this Block Diagram can be explained with the help of two user's ALIES, BOB. If we navigate through user ALIES, we would understand the process of encryption of secret information into a encrypted video file. Similarly, If we navigate through user BOB. We would understand the process of decryption of secret information from a encrypted video file.

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

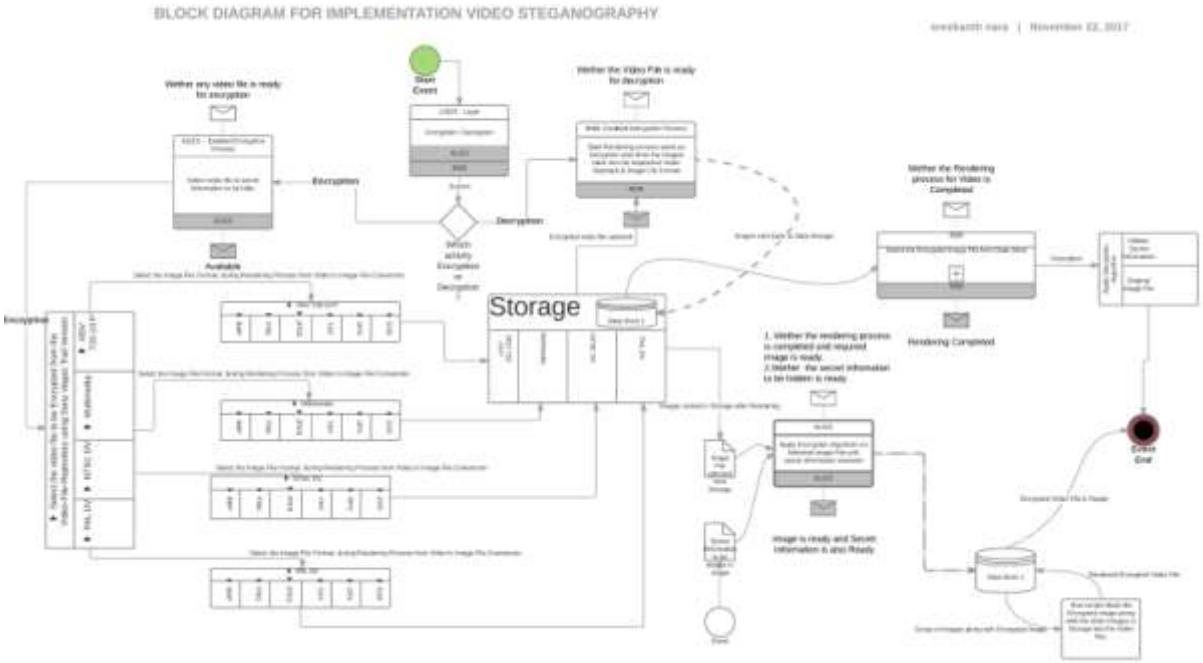

Figure 1.2:- System architecture for implementation of Video Steganography.

The popular video standards support by selected resolution and Image File Format explored for experiment can be known from **Table 1.2 – Popular Video Standard used in Sony Vegas 9.x software** as given below.

Video-Standard	**Image File Type**						
		BMP	**JPEG**	**PNG**	**TIFF**	**DPX**	**EXR**
	HD 720-24	Yes	Yes	Yes	Yes	Yes	Yes
	Multimedia	Yes	Yes	Yes	Yes	Yes	Yes
	NTSC DV	Yes	Yes	Yes	Yes	Yes	Yes
	PAL DV	Yes	Yes	Yes	Yes	Yes	Yes

Table 1.2 : Popular Video Standard used in Sony Vegas 9.x software Trail version.

II. EXPERIMENTAL SETUP

For information gathering we need the following application software - Video Editing Tool: Sony Vegas Pro 9.0, any P-IV configuration PC, but recommended Hard Disk Drive should have minimum 500GB. Why I am more specific about the HDD? Because this application software generates more number of images of same type for a given resolution set, but May or may not vary in file size depending on the type of file format. As a sample, we have selected a video clip of about 74 seconds. In the above mentioned application software, we have many option to play with video clip. For this experiment we are using an option 'render as' were the video clip can be converted into images of our choice. Example: BMP, DPX, PNG, JPEG, WMPHOTO, EXR and TIFF. Adding to this it also has an option to select different video standards.

2.1 DIFFERENT-IMAGE-GENERATOR ALGORITHMS

Using Song Vegas Pro 9.0 Tool, The navigation steps for generating images process are given below:

A. From the **File menu**, choose **New**. New Project Window is popup

B. Enter your project setting on the various tabs.

B.1. **Video Tab** : It allows you to select the video format and other video parameters like fps , resolution etc.,

B.2. Audio Tab : It allows you to set up the basic audio settings

B.3. Ruler Tab : It allows you to choose the way the ruler is delineated {beats , seconds ,etc}

B.4. Summary Tab: It allows you to enter any relevant information and reminders about your project.

B.5. Audio CD: It allows you to enter information for burning audio CDs.

Note: In our case we select only the Video Standard.

C. Click ok

D. From the **File menu**, choose **Save**. Enter a name , browse for a location ,and click save to save your project{vet file}

Note: We can change project settings at any time while working on a project. From the File menu, choose Properties to change any of these settings.

E. Adding media to the Project Media List from the Explore Window.

E.1. Navigate to and select a file (video clip of 74 sec) to add to the Project Media List.

E.2. Right –click the file and choose Add to Project Media List from the shortcut menu. The selected file is added to the Project Media List.

F. Create folders related to the image file name to store all the images into that particular folder.

G. From the **File menu**, choose **Render As**. The **Render As** dialog appears

H. From the **Save in** drop-down list, choose the drive and folder where the file will be saved.

I. Enter the new name for the project In the **File name** box.

J. From the **Save as type** drop – down list, choose the desired file format.

K. From the **Template** drop-down list, choose the multiple mono templates, or choose an appropriate 5.1 channel template if selected file type supports it.

L. Select the **Render loop region only** check box if you want to save only the portion of the project that is contained within the loop region.

M. If the selected file type supports it, you can select the **Save project makers with media file** check box to include makers, regions and command makers in the rendered media file.

N. Click **Save**. A dialog is displayed to show rendering progress.

O. When rendering is complete, click the **Open** Folder to open the folder where you saved the file.

P. Repeat G until we gather each type of image format in their respective folders.

Q. Repeat B until we gather each type of video standard as mentioned below.

R. Stop

Through this algorithm specific image file type is generated in respective image folder for all the video standards we have opted. Now, we should tabulate information about the image file type by observing each folder. Each folder, it illustrate the information about each image file type like minimum file size , maximum file size , No. of Frames, variation in size for different frames, render time and total size of folder. This a different approach when compared with references[18,19,20].

2.2 TABULATING DIFFERENT TABLES BASED ON DIFFERENT VIDEO STANDARDS:

2.2.1 MULTIMEDIA – 320 X 240, 29.970 FPS:

This video standard uses resolution 320 x 240 with approximately 30 frames per second. Through this one can achieve clarity in motion, but if viewed in large screen, it would affect with blurriness it also consist of more number of frames. The advantages of using this video standards is that it consumes less space and also it takes less time for gathering the information, which can be noticed through the "Render as time" column.

Table 2.2.I (Multimedia – 320 x 240, 29.970 fps):

File Type	Min (KB)	Max (KB)	Diff – in (KB)	No. of Frames	Render as time Mm:ss	Size of the folder
BMP	301	301	-	3234	01:31	0.98GB
DPX	233	233	-	3234	07:20	808MB
PNG	44	140	96	3234	01:02	382MB

JPEG	6	20	14	3234	00:35	101MB
TIFF	75	180	105	3234	00:51	507MB
EXR	60	167	107	3234	03:30	457MB

2.2.2 NTSC DV –655 X 480, 29.970 FPS:

This video standard uses resolution 655 x 480 with approximately 30 frames per second. This video standard is better than Multimedia – 320 x 240, 29.970 fps, as the resolution is better in this case and rest of the feature are same. But has the limitation like it requires,more storage space and takes more time to gather the information.

Table 2.2.II (NTSC DV –655 x 480, 29.970 FPS):

File Type	Min (KB)	Max (KB)	Diff – in (KB)	No. of Frames	Render as time Mm:ss	Size of the folder
BMP	1229	1229	-	3234	05:06	3.84GB
DPX	931	931	-	3234	08:57	2.96GB
PNG	153	520	367	3234	02:50	1.19GB
JPEG	15	49	34	3234	01:03	139MB
TIFF	286	695	409	3234	01:57	1.74GB
EXR	170	539	369	3234	12:06	1.22G

2.2.3. PAL DV – 1049 X 576, 25 FPS:

This video standard uses resolution 1049 x 576 with 25 frames per second. Even though the number of frames are less it consumes more space mainly due to high resolution and also it takes pretty good time to gather the information ,when compared with the above two video standards.

Table 2.2.III (PAL DV – 1049 x 576, 25 fps):

File Type	Min (KB)	Max (KB)	Diff – in (KB)	No. of Frames	Render as time Mm:ss	Size of the folder
BMP	2361	2361	-	2698	08:07	6.09GB
DPX	1779	1779	-	2698	08:29	4.61GB
PNG	253	746	493	2698	03:35	1.41GB
JPEG	24	66	42	2698	1:33	159MB
TIFF	498	1023	525	2698	02:52	2.15GB
EXR	259	739	480	2698	15:43	1.39GB

2.2.4. HDV 720 – 24P – 1280 X 720, 23.976 FPS:

Among all the standards listed above, I would consider this video standard to be the best of its kind for the case of high resolution, where the image clarity is really very good. But suffers with limitation like worst in consuming more space, takes more time in gathering the information.

Table 2.2.4 (HDV 720 – 24P – 1280 x 720, 23.976 fps):

File Type	Min (KB)	Max (KB)	Diff – in (KB)	No. of Frames	Render as time Mm:ss	Size of the folder
BMP	3601	3601	-	2587	15:27	8.92GB
DPX	2708	2708	-	2587	09:21	6.71GB
PNG	355	1119	764	2587	06:02	1.94GB
JPEG	33	90	57	2587	01:46	185MB
TIFF	717	1562	845	2587	04:37	3.10GB
EXR	351	1055	704	2587	23:03	1.84GB

III. PRE-ENCRYPTION PROCESS

For selecting, the optimistic image file format, which best suits Image Steganography we known compare the file size one by one for a specific Image File type, with the help of creating Master Comparison Table from various Tables tabulated using different Video-Standard. The video standards have been selected based on regular usage. In this master table consists of only Min, Max & Diff columns. The data obtained here is before inserting secret information into the image. The purpose of selecting only these three columns is that in the initial stage, the software is able to generate more number of images with different sizes. For getting optimistic image file type, we should always select an image from the video standard which has greater difference or atleast minimum difference, But not an image without any difference, Because consider a secret information whose size is atleast 10KB. When this secret information is embedded with a selected image file type, then obviously the image file size would vary. And vice-versa when we want to locate the image file which consists of hidden secret information then by observing the image file size it would be easy to locate it provide we known the standard file size for various image file format for different resolution.

3.1 Master Comparison Table for Various Video-Standard

Master Comparison Table For Various Video-Standard					
SL.NO	**FILE TYPE**	**VIDEO STANDARD**	**MIN (KB)**	**MAX (KB)**	**DIFF (KB)**
1	**BMP**	**MULTIMEDIA – 320 X 240, 29.970 FPS**	301	301	-
		NTSC DV –655 X 480, 29.970 FPS	1229	1229	-

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Master Comparison Table For Various Video-Standard					
		PAL DV – 1049 X 576, 25 FPS	2361	2361	-
		HDV 720 – 24P – 1280 X 720, 23.976 FPS	3601	3601	-
2	**DPX**	**MULTIMEDIA – 320 X 240, 29.970 FPS**	233	233	-
		NTSC DV –655 X 480, 29.970 FPS	931	931	-
		PAL DV – 1049 X 576, 25 FPS	1779	1779	-
		HDV 720 – 24P – 1280 X 720, 23.976 FPS	2708	2708	-
3	**PNG**	**MULTIMEDIA – 320 X 240, 29.970 FPS**	44	140	96
		NTSC DV –655 X 480, 29.970 FPS	153	520	367
		PAL DV – 1049 X 576, 25 FPS	253	746	493
		HDV 720 – 24P – 1280 X 720, 23.976 FPS	355	1119	**764**
4	**JPEG**	**MULTIMEDIA – 320 X 240, 29.970 FPS**	6	20	14
		NTSC DV –655 X 480, 29.970 FPS	15	49	34
		PAL DV – 1049 X 576, 25 FPS	24	66	42
		HDV 720 – 24P – 1280 X 720, 23.976 FPS	33	90	**57**
5	**TIFF**	**MULTIMEDIA – 320 X 240, 29.970 FPS**	75	180	105
		NTSC DV –655 X 480, 29.970 FPS	286	695	409
		PAL DV – 1049 X 576, 25 FPS	498	1023	525
		HDV 720 – 24P – 1280 X 720, 23.976 FPS	717	1562	**845**
6	**EXR**	**MULTIMEDIA – 320 X 240, 29.970 FPS**	60	167	107
		NTSC DV –655 X 480, 29.970 FPS	170	539	369
		PAL DV – 1049 X 576, 25 FPS	259	739	480
		HDV 720 – 24P – 1280 X 720, 23.976 FPS	351	1055	**704**

3.2 STANDARDIZING FILE SIZE FOR IMAGE FILE TYPE

If, we create a comparison chart for the above Master Comparison Table for Various Video-Standard, Here one thing, that it would clarify is for image file type **BMP & DPX** even though it generates more number of images of same resolution, the file size is same. So from this experiment we setup standards for BMP & DPX.

Sl. No	File Type	Video Standard	File Size (KB)
1	**BMP**	**Multimedia – 320 x 240, 29.970 fps**	301
		NTSC DV –655 x 480, 29.970 fps	1229
		PAL DV – 1049 x 576, 25 fps	2361

		HDV 720 – 24P – 1280 x 720, 23.976 fps	3601
2	**DPX**	**Multimedia – 320 x 240, 29.970 fps**	233
		NTSC DV –655 x 480, 29.970 fps	931
		PAL DV – 1049 x 576, 25 fps	1779
		HDV 720 – 24P – 1280 x 720, 23.976 fps	2708

3.3 NON-STANDARDIZING FILE SIZE FOR IMAGE FILE TYPE

But, we cannot makeup standards for other Image File Type's like **PNG / JEPG / TIFF / EXR etc.,** as it varies from image to image even though the resolution is same. So, Now we have to see if the file size is constant for BMP & DPX after embedding the secret information into the selected image file type.

IV.POST-ENCRYPTION PROCESS

For encryption, we have used readily available Image-Steganography program written in java code available on internet. After embedding secret information into the image file type and upon observing the file size it was clear that there is variation in the file size for BMP File type. Now, we would conclude that BMP is not the best suitable image file type. As already we have setup some standards which have revealed what would be the image file size for a given resolution. It's easy for a user to recognize, if the image file type has any hidden information by observing the file size, no need of any cryptographic algorithm for it. But, it would be required to decrypt, the secret information within that particular image file type.

V. RESULTS

If we draw the Column Chart for the above **Master Comparison Table for Various Video-Standard** would be as shown below:

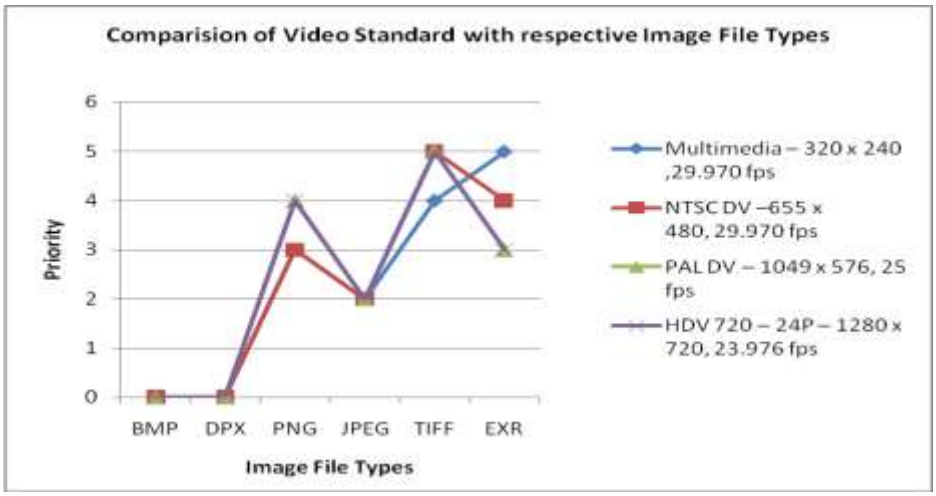

FIGURE 5: Comparison of Video Standard with respective Image File Types

Finally, our conclusions based on the selected four video standards are as follows:

In the Figure 5 on the X-Axis it specifies the type of image file format and on the Y-Axis it specifies the priority of selection of the Image File format and for video standards the color is different and representation is also different. For instance, if we look at PNG image file format among the video standards listed the best one could be HDV 720 – 24 P – 1280 x 720, 23.976 fps.

The priority of selection of image file type can be concluded as mentioned below in Table 5.1:

Video-Standard	**Image File Format**						
		BMP	**JPEG**	**PNG**	**TIFF**	**DPX**	**EXR**
	HD 720-24	weaker	stronger	stronger	stronger	weaker	stronger
	Multimedia	weaker	weaker	weaker	weaker	weaker	weaker
	NTSC DV	weaker	average	average	average	weaker	average
	PAL DV	weaker	moderate	moderate	moderate	weaker	moderate

Table 5.1 :A Weaker to Stronger Image File Format selection for implementing Image Steganography

i.First recommended image file format would be TIFF for implementing Image Steganography, except only if the case of video standard is HDV 720 -24P-1280x720 , 23.976 fps.

ii.Second recommended image file format would be EXR for implementing Image Steganography.

iii.Third recommended image file format would be PNG for implementing Image Steganography.

iv.Fourth recommended image file format would be JPEG for implementing Image Steganography.

v.The wrong selection of choice would be BMP | DPX for implementing Image Steganography.

VI.CONCLUSION

Our conclusion from these experiment results, we have considered only file size. But, nevertheless there are some other parameters like resolution to be considered, as there are directly proportional.

Achieved: Selecting Optimistic Image File Type α File Size

Future work, we want to conduct some experiments to solve, how image resolution affects the file size in some image file types like TIFF, EXR, PNG, JPEG.

Unachieved: File Size α Image Resolution

REFERENCES

[1]: Sreekanth Nara, Dr M.H.M. Krishna Prasad, Ravindra Changala. Exploiting the Vulnerabilities of Image Steganography through Hacking Tools, IJETED Issue 2, Vol.4 (May 2012) ISSN 2249-6149.

[2] Farid, H. Detecting Steganographic Messages in Digital Images. Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001.

[3]Farid, H. and Lyu, S. Higher-order wavelet statistics and their application to digital forensics. *IEEE Workshop on Statistical Analysis in Computer Vision*, Madison, Wisconsin, June 2003.

[4]Fridrich, J. and Du, R. Secure steganographic methods for palette images. In: *Proceedings of the 3rd Information Hiding Workshop*, Lecture Notes in Computer Science, vol. 1768. Dresden, Germany, September 1999. Springer-Verlag, Berlin, Germany, 2000, pp. 47-60.

[5]Fridrich, J. and Goljan, M. Practical steganalysis of digital images: State of the art. In: *Proceedings of th e SPIE Security and Watermarking of Multimedia Contents IV*, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, 2002, pp. 1-13.

[6]Fridrich, J., Goljan, M., and Du, R. Steganalysis based on JPEG compatibility. In: *Proceedings of the SPIE Multimedia Systems and Applications IV*, Special Session on Theoretical and Practical Issues in Digital Watermarking and Data Hiding, vol. 4518. International Society for Optical Engineering, Denver, Colorado, August 21-22, 2001, pp. 275-280.

[7] Curran, K. and Bailey, K. An evaluation of image-based steganography methods. *International Journal of Digital Evidence* [Online]. (Fall 2003).

[8]Jackson, J. T., Gregg, H., Gunsch, G. H., Claypoole, R. L., and Lamont, G. B. Blind Steganography detection using a computational immune system: A work in progress. *International Journal of Digital Evidence* [Online]. (Winter 2003) (December 21, 2003).

[9]Johnson, N. F., Duric, Z. and Jajodia, S. *Information Hiding: Steganography and Watermarking: Attacks and Countermeasures*. Kluwer Academic, Norwell, Massachusetts, 2001.

[10]Johnson, N. F. and Jajodia, S. Exploring steganography: Seeing the unseen, *Computer* (1998A) 31(2):26-34.

[11]Johnson, N. F. and Jajodia, S. Steganalysis of images created using current steganography software. In: *Proceedings of the Second International Workshop on Information Hiding* (IH '98), Lecture Notes in Computer Science, vol. 1525. D. Aucsmith, ed. Portland, Oregon, April 14-17, 1998. Springer-Verlag, Berlin, Germany, 1998B, pp.273-289.

[12] Abhishek Mangudkar, Prachi Kshirsagar, Vidya Kawatikwar, Umesh Jadhav Data Hiding Technique using Steganography and Dynamic Video Generation , International Journal of Scientific & Engineering Research , Volume 3 , Issue 6, June 2012 ISSN 2229-5518

[13] Armin Bahramshahry, Hesam Ghasemi, Anish mitra, and Vinayak Morada., "Design of a Data Hiding Application using Steganography(April 2007)

[14] J.Siegfried, C.Siedsma, B.J. Countryman, C.D. Hosmer, "Examining the Encryption Threat," International Journal of Digital Evidence, Vol.6, pp. 23-30, December 2004

[15] A. Stubblefield, J.Ioannidis, A.D.Rubin, " A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)," ACM Transactions on Information and System Security, Vol. 7, pp. 319-332, May 2004

[16] R.Chandramouli, N.Memon, "Analysis of LSB based image Steganography techniques, "Image Processing, Vol. 3, pp. 1019-1022, October 2001

[17] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier" Journal of Global Research in Computer Science, Vol. 2, No. 4, April 2011. ISSN-2229-371X

[18] Amr A.Hanafy, Gouda I. Salama and Yahya Z. Mohasseb. The Military Technical College, Cairo, Egypt 11331, " A Secure Convert Communication Model Based On Video Steganography", 978-1-4244-2677-5/08/$25.00@ 2008 IEEE

[19] N. Provos and P.Honeyman, "Hide and Seek : An Introduction to Steganography", IEEE Security & Privacy Magazine, Vol. 1, issue 3, pp. 32-44, June 2003.

[20] Hema Ajetrao, Dr.P.J.Kulkarni and Navanath Gaikwad, " A Novel Scheme of Data Hiding in Binary Images", International Conference on Computational Intelligence and multimedia Applications, Vol. 4 , pp. 70-77, Sivakasi Tamil Nadu, Dec. 2007.

[21] Derek Upham. Jsteg, http://zooid.org/~paul/crypto/jsteg/..

[22] Allan Latham. Jphide, http://linux01.gwdg.de/~alatham/stego.html.

[23] K. Solanki, A. Sarkar, and B. S. Manjunath. Yass: Yet another steganographic scheme that resists blind steganalysis. In Proceedings of the 9th Information Hiding Workshop, volume 4567 of LNCS, pages 16{31. Springer,2007.

10. AUTHORS:

Mr. Sreekanth Nara received Master of Technology in Computer Science Engineering from School of Information Technology, Jawaharlal Nehru Technological University (JNTUH) and pursuing PhD from Rayalaseema University, Kurnool. His research interests include Multimedia Security, Data Mining. He is a Member of ACM since 2010 and also a Member of CSI.

Dr. M.H.M. Krishna Prasad, received Ph.D from JNTUK, offered Fellowship (U.of Udine, Italy) for Ph.D, and received Master of Technology in Computer Science Engineering from Jawaharlal Nehru Technological University (JTNUH). His research interests include Data Mining and Multimedia Security. Presently working as Associate Professor & Head Dept. of Information Technology University College of Engineering JNTUK –Vizianagaram Campus Vizianagaram, Andhra Pradesh, India.