JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Analysis of Different Image Formats for Steganography

Prof. VaidyaKrishna[1]
Research Scholar
Saurashtra University, Rajkot, India
Krishnavaidya1991@gmail.com

Prof. (Dr.) C K Kumbharana Co-Author[2]
HOD, Computer Science Dept.
Saurashtra University, Rajkot, India
ckkumbharana@yahoo.com

Abstract:

To avoid detection of hidden data, a technique named steganography is used. Transfer of confidential data secretly is the aim of steganography. Discussion of different image formats (like BMP, JPEG, PNG Etc.) for the steganography is presented in this paper. Technical properties, application and limitation of steganography will also be discussed here.

Keywords: Steganography, Image Steganography File Format, JPEG, PNG, BMP.

INTRODUCTION

Nowadays transfer of data is increased hence, security of the data is crucial point at this time. To decrease risk of attack throughout transmission, steganography method can be helpful in that scenario as per the current trend. Here cover objects can be used for hiding data. All type of cover objects can be used for steganography. Cover objects like Image, Audio, Video and text is used. Cover object is chosen based on degree of redundancy. The more redundancy , the more data can be hide in that. Therefore, out of all cover objects images are more popular. However, text steganography is not used mostly due to its smaller number of redundant data in it. Audio and Video steganography are little complex as compared to image, so they are not much in use. In which we hide the data is called cover image. Data bind with hidden data using some steganography algorithm and secret key is called stego image as shown in Fig. 1.

An analysis of different image formats for steganography is presented by this paper. The organization of paper is as follows: Technical properties, applications and limitation of steganography is included in Section 1. Section 2 includes Steganography cover image formats and color model information. In Section 3, Literature Review of different image formats are presented. An analysis of different image formats is presented in Section 4. At last, in Section 5, conclusion is described.

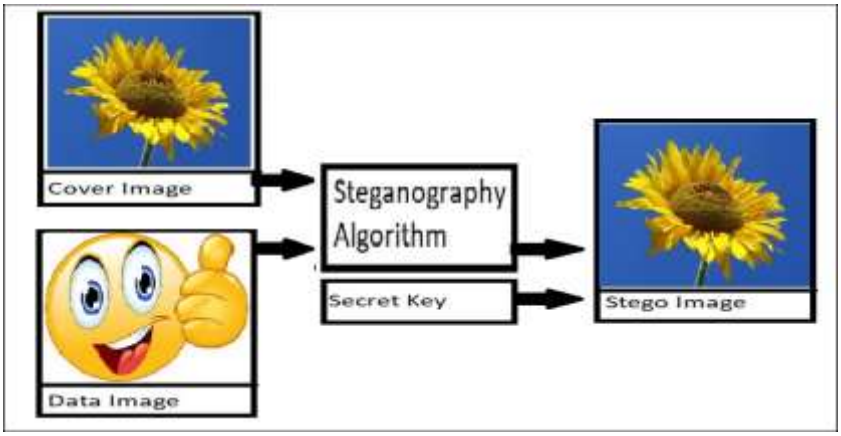

Figure 1. Image Steganography Example

Steganography can be used in many applications like Governmental, Scientific and Social applications. Everything in the world has some limitations. Hence, steganography has also some limitations. Steganography can be misused. Steganography has some problems for using it. Following are some limitations and applications of steganography.

Limitations of Steganography

- To damage the security of data, attackers use steganography. Example : from social media one can steal somebody's personal information. Copy illegally of software or films can also be generated through it.
- Illegal activities can be done by terrorist using steganography. To prevent from such issues, government has taken some steps to stop it. Therefore, Steganography is always under high observation.

Applications of Steganography

- Top-secret locations can be transferred through steganography.
- Confidential information can be passed through it.
- For the secure online voting, it can be used.
- Steganography can also be used for secure communication for the military purpose.
- It can also be used for secure ecommerce transactions.
- It can also be used for verification purpose.
- It can be used by police department and detective investigation department.

I. COVER IMAGE FORMATS FOR STEGANOGRAPHY

Here we will be discussing different image formats and their color models for steganography. Different characteristics are conceived by different image formats. Moreover, all the image formats include header information as well. Main difference between all of them is amount of compression of data into them. Example, 9.6 mb of storage is needed by RGB color image of 24 bits without any compression. But lesserspace is occupied by it for compression. If more compression is done then, it can be chances of loss of data. BMP, PNG and TIFF have lossless property. Whereas JPEG has lossy property.

A. JPEG (Joint Photographic Experts Group)

It is most popular Image format. Digital cameras, memory cards, web pages and image processing use this format for better compression of file and less risk of attack on it. Main disadvantage of JPEG is lossy property. Repeatedly image edition is not allowed here, due to the risk of loss of data. It creates small file due to its lossy property. It has good transfer speed. It also supports true color image.

Table 1. JPEG File Structure with Header Fields [1].

Header Field for JPEG	Size
Image_Width	512
Image_Height	512
Image_Components	3
Image_Color_Space	2
Jpeg_Components	3
Jpeg_Color_Space	3
Comments	{}
Coef_Arrays	{1x3 cell}
Quant_Tables	{[8x8 double] [8x8 double]}
Ac_Huff_Tables	[1x2 struct]
Dc_Huff_Tables	[1x2 struct]
Optimize_Coding	0
Comp_Info	[1x3 struct]
Progressive_mode	0

B. BMP (Bitmap)

It offers two modes: grey scale and color mode with compressed and uncompressed file formats. Transparency property is also supported by it. Maximum 256 colors per pixel is used in 8-bit bitmap. It has 16 bits, 24 bits, 36 bits and 48 bits format. Image format of 48 bits has more color depth because in its each R, G and B channel 16 bits are used. 8 bits are used each channel of 24 bits format and brightness value is between 0 and 256. In 16 bits format, 2 bytes are used for each pixel. Header information for BMP is as follows and detail about it is given in following table 2 [26].

BITMAPFILEHEADER (Bitmap File Header) → bmfh;
BITMAPINFOHEADER (Bitmap Information Header) → bmih;RGBQUAD
(Array of Bitmap Bits for color table) → aColors[];
BYTE (Bitmap Bits contains array of Bytes for describing rows) → aBitmapBits[];

Table 2. Bitmap File Structure.

Bitmap Structure Field	Information
Bmfh;	Field Byte, Size and Layout of a Device is described here. Here Bitmap File is Independent.
Bmih;	Here compression type, dimensions and color format are describer for bitmap format.
aColors[];	Here basic color elements for color array are described. Scan line stored in bitmap is represented by number of bytes. Lower-Left side bitmap are represented by first byte of array. Moreover, Upper-Right side bitmap are represented by last byte of array.
aBitmapBits[];	Maximum number of 256 colors are contained by 8-bit Bitmap. 1 Byte is represented by each pixel in color table. Whereas 2^24 colors are contained by 24-bit Bitmap. For a pixel , Intensity of each Red, Green and Blue is represented by each 3-byte sequence.

C. PNG (Portable Network Graphics)

If we want to maintain original quality for a smaller file then PNG Format is used. Its main use is to transfer image on internet. It supports different degree of transparency and multiple colors. Image can be to background image due to transparency property of it. Indexed color, Grey Scale and RGB is supported by PNG Format. Palette based image for 24-bit and 32-bit is supported here. The data compression used here is lossless. Here first compression is done and then data is stored, Hence, resolution is properly maintained here. Here Signature value of 8-byte is as presented in Table 3, which is having field value in hexadecimal and chunks of 4 parts is presented in Table 4.

Table 3. 8-Byte Signature of PNG

Field Value (In Hexadecimal)	Description
89	Here transmission system is identified through high bit. Here 8-bit is not supported. Here it can also happen that text file is considered as PNG and vice versa.
50- 4E – 47	Here format can be identified individually without any problem. For that text editor is used.
0D – 0A	Line ending conversion is identified in DOS / UNIX.
1A	Display of file can be halt in DOS, when end of file character is detected.
0A	Here Unix line ending is used to detect conversion of end of line.

Table 4. PNG Chunks

Value Length	Chunk Type	Chunk Data	CRC Length
4 Bytes	4 Bytes	Length Bytes	4 Bytes

D. TIFF (Tagged Image File Format)

It is developed by Aldus Corporation in 1986. In one file , it can incorporate many images. It is lossless compression, so resolution is maintained here. Here repeatedly editing is allowed without any loss of data. It can be used with photo manipulation software like photoshop, which offers many options like tags, layers and transparency. If one wants to edit digital image then this format is best choice. Grey scale, palette-color and RGB full color-image is supported here.

Color Models

Here range of colors are created from basic color. In image processing , RGB and CMYK are popular. Brief description of some color models are as follows.

1) **CMYK Model :** Full form of CMYK model is cyan-magenta-yellow-black. Here printing ink is used, due to reflection of light, colors are produced.

2) **RGB Model :** Full form of RGB model is red-green-blue. Here colors are presented with the help of light. Light + different colors will make variety of colors. It is mainly used for images of computer and TV. It is additive color model. RGB model used by BMP format mostly.

3) **HSV Model :** Full form of HSV model is hue-saturation-value. Tone is the meaning of hue. here also lightening is used with combination of shades and brightness value of color. Color editing software uses it mostly. However, it is not used in image analysis. 0 to 360 degree is range of (h) color type. 0 to 100% is color range of (s) and (v). (v) means value of brightness. (s) means shade of color. HSB model is same as HSV.

4) **HSL Model :** Full form of HSL model is hue-saturation-lightness. It is same as HSV model. Here color is represented in 3-D view. Here entire brightness range of value's span is wide.

5) **NCS Model :** Full form of NCS model is natural-color-system. Here six colors are used. They are white, black, red, yellow, green and blue.

6) **Indexed Color :** Here number is used to represent the color. And numbers are indexed with different colors corresponds to them in color table (palette).

III. LITERATURE REVIEW OF DIFFERENT IMAGE FORMATS

Different Image formats for the steganography are reviewed from the different research papers. Review of the research paper are given in tabular form according to different formats like JPEG, BMP and PNG. Table describes different methodology used for different formats.

Table 5. Image Steganography algorithms using JPEG Format

Reference	Methodology	Data Used
Hamidreza Et al [2]	Here distortion is reduced using DCT Method. They adjusted the cost value for minimizing distortion. Due to proposed algorithm performance and security increased.	3 different Sample cover images of magnetic resonance imaging used for testing of algorithm.
Deepa shankar Et al [3]	It focuses on steganalysis. Here they have combined 4 techniques : LSB Matching & Replacement, PVD and F5. Support Vector Machine is used for classification.	2 Databases are used : INRIA and UCID.
Vaclav Snasel Et al [4]	To improve property of image, optimization is used here. However, complexity can also be added due to optimization. Here performance is increased of algorithm.	3 Images nearby of 9000 bytes are taken into consideration for testing of their proposed algorithm.
Lalit Gupta Et al [5]	Here LSB technique implemented in OpenPuff Steganography tool. Different parameters are analyzed here like : PSNR, Extraction Time, Hiding Time Etc.	10 images taken for testing of algorithm in countersteg tool.
Jie Wang Et al [6]	Payload location is detected first. It divides into sub-images and then filter from that images. Two algorithms are used : Jsteg and F5.	2 images are taken. 1 for cover image that is lena.jpg and other for hidden image.

Table 6. Image Steganography Algorithms using BMP Image Format

Reference	Methodology	Data Used
Istteffanny Araujo Et al [7]	They have tried to improve capacity and minimize the distortion and detectability using their proposed algorithm. Extra security added using RSA Algorithm.	1 BMP image is used with other image formats for comparison.
Khaldi Amine [8]	Author came to conclusion that not any single method for all image formats exists. As all image formats have their individual characteristics.	Only classification of Image Formats.
Aamer Tahseeen [9]	Here circular secret key is created at random. Detection of secret data is difficult using proposed algorithm.	Testing of image is not presented in this paper.
S Hardi Et al [10]	LSB Method is used with RGB Image. Cryptography is also used for extra security. They have increased size of key, so that it is difficult to detect. However, execution time is long here.	Single image of 5760 x 3840 is tested for their proposed algorithm.
D Magomedova Et al [11]	Algebraic Fractals are used here. Due to this approach integrity and authenticity is increased.	Color image of 2560 x 1440 is used for testing. Different fractal cover images also used.

Table 7. Image Steganography Algorithms using PNG Image Format

Reference	Methodology	Data Used
D Darwis Et al [12]	Different Image steganography methods compared like LSB, PVD and MF. Out of all this, they came to conclusion that LSB is best for quality. PVD is best for capacity.	Gray scale and RGB image of 512 x 512 is used. Total 7 images tested.
Farrukh Abbas [13]	Blowfish algorithm + Pixel indicator technique is used for improving security.	Basic 4 images taken into consideration for testing.
Arshiya Ansari Et al [14]	Here data are pre-estimated, double encryption at hidden location and data are scattered. Clustering method is used.	Lena, pepper, baboon, moon (512x512), doll and blue sky(480 x480), garden(544x544), cats(456x448) images are used for testing.
Dr Archana Gupta [15]	Description of PNG Format is given. PNG format is good for LSB method.	Only comparisons between image formats. No testing of images is presented.
Zhiqing Lu Et al [16]	Neural Network and Scale compression both are combined here. Proposed algorithm gained performance.	Total 7 images (baboon, house, jet, peppers, sailboat, splash, tiggany, Lena) of 512x512 presented for testing.

IV. ANALYSIS

Here we have done analysis of some of the image steganography methods for different file formats. Main purpose of analysis is to test different image formats compatibility in different image steganography methods. It will help researcher to compare different image formats for various image steganography methods.

Here some parameters are used for analysis of image steganography methods, parameters like technical properties, perceptibility and security are used.

High quality is determined through high PSNR. Good quality stego image is considered through above 40db PSNR. Table 8, Table 9 and Table 10 shows PSNR values for different image steganography methods of various image formats. Fig. 2, Fig. 3 and Fig. 4 presents comparisons of image formats in different image steganography methods through chart. Here we have selected 2 images as cover image. They are Lena and Baboon using BMP / PNG / JPEG image formats.

Comparison of JPEG as coverimage is shown in Table 8 and Fig. 2. 4096 bits of data are used as secret data in method [17], whereas 35,160 bits of data used in method [1]. It has higher PSNR & secret data than method [17]. PSNR for BMP images shown in Table 9 and Fig. 3 [18][19][20][21]. Amongst all methods [19] has good PSNR forboth images. PSNR for PNG images shown in Table 10 and Fig. 4 [22][23].

Fig. 5 shows difference of PSNR value in different image formats. From the Fig. 5, it is clear that PNGhas deprived quality and can store less amount of secret data. Good capacity and security are provided through JPEG. Higher capacity and PSNR is achieved through BMP. Table 11 shows PSNR comparison between different image formats. Table 12 provides performance analysis of different image formats. It will be clear from the table that some method uses hybrid concept. However, hybrid provides good security but it is complex. From the table 11 we can summaries following points:

- Less capacity and security provided through PNG Image format.
- Best capacity is provided through JPEG, out of all Image formats. However, it is complex thanother Image formats.
- High capacity and security provided through BMP Image format as well.

Table 8. Different Steganography method's PSNR (in dB) comparison using JPEG Image Format

Sr. No.	**512 x 512 Cover Image**	**Coefficients Method** [1]	**RDHS Method** [17]	**APVD Method** [24]	**TQWT Method** [25]
1	Lena	59.74	47.27	50.89	41.69
2	Baboon	59.75	31.05	52.29	31.92

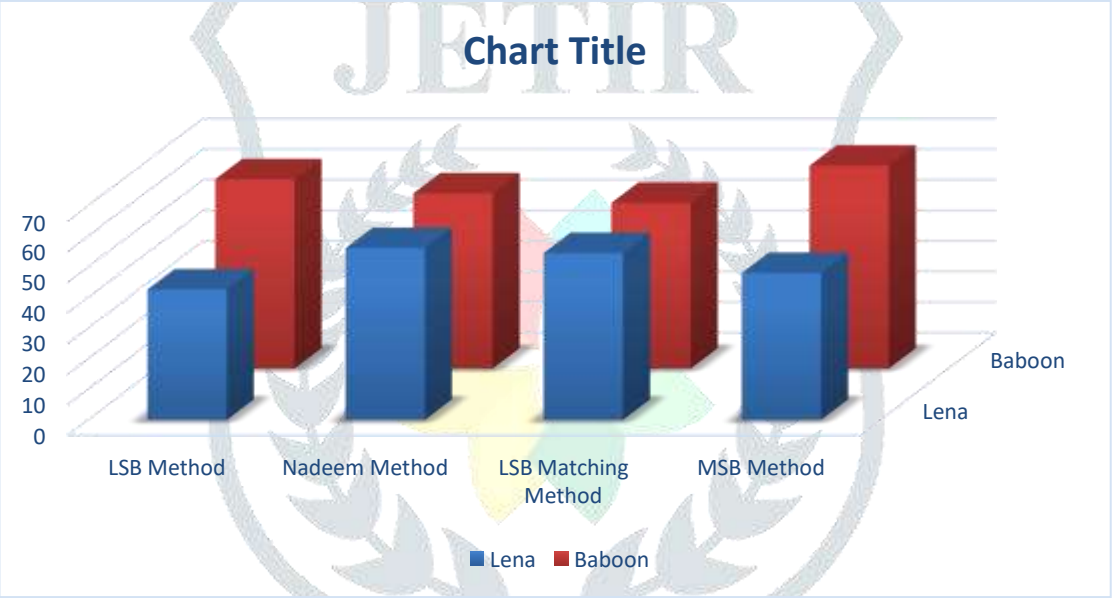

Figure 2. PSNR comparison of various method using JPEG.

Table 9. PSNR (in dB) comparison for different steganography methods of BMP cover image

Sr. No.	**512 x 512 Cover Image**	**LSB Method** [18]	**Nadeem Method** [19]	**LSB Matching Method** [20]	**MSB Method** [21]
1	Lena	42.63	56.12	54.53	48.00
2	Baboon	61.87	57.26	54.15	66.28

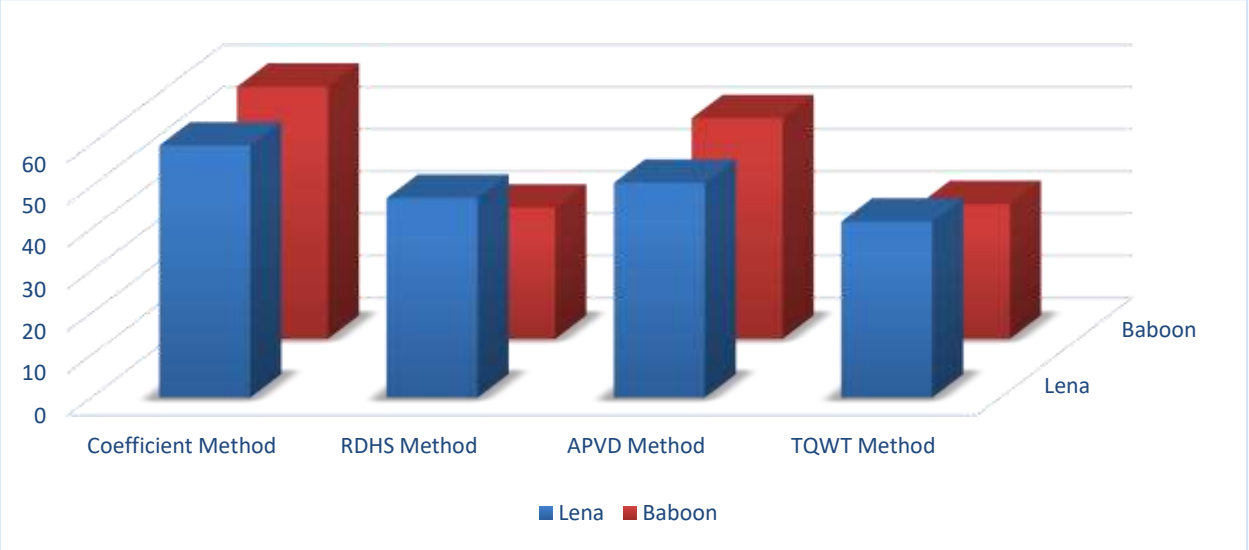

Figure 3. PSNR comparison for BMP Image format

Table 10. PSNR (in dB) comparison for different steganography methods of PNG cover image

Sr. No.	512 x 512 Cover Image	Rojali Method [22]	Yung Method [23]	EZ-stego Method [23]	Fridrich Method [23]
1	Lena	51.30	36.95	14.23	31.28
2	Baboon	51.80	35.86	14.55	30.64

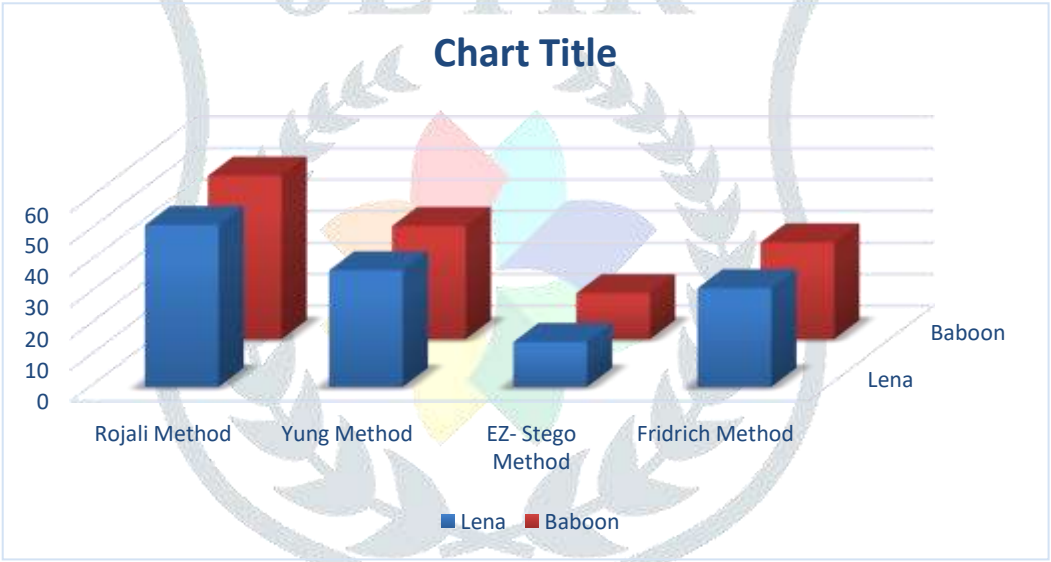

Figure 4. PSNR comparison for PNG image format

Table 11. PSNR comparison between JPEG , BMP and PNG Format

	Lena	Baboon
JPEG	49.89%	43.75%
BMP	50.32%	59.89%
PNG	33.44%	33.21%

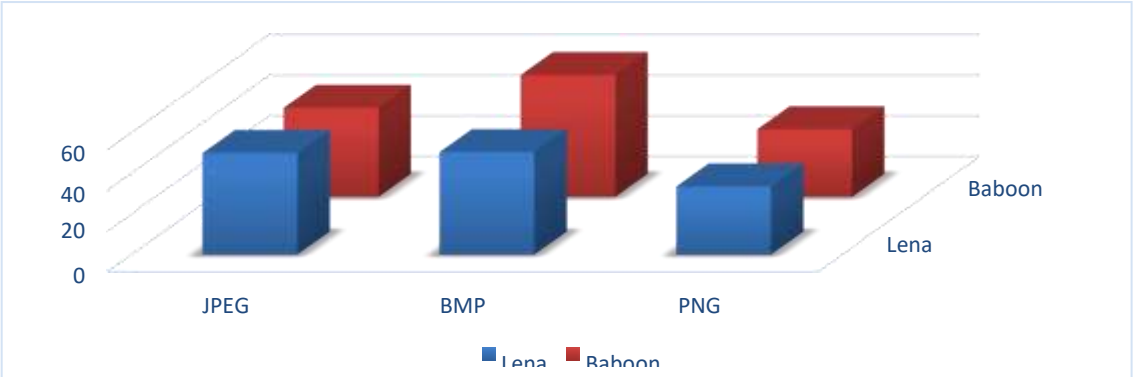

Figure 5. PSNR comparison of different Image Formats

Table 12. Performance analysis of JPEG, BMP and PNG

Formats / Properties	JPEG	BMP	PNG
Lossless Compression	Low	High	High
Transparency	Low	Low	High
Color Bits	24	32	24.48
Hiding Timing	High	Low	High
Extracting Timing	Low	High	High
File Size	Low	High	High
Confidentiality	Medium	High	Medium

V. CONCLUSION

Different image steganography method's performance recorded from 2014 to 2021 year's publication. Analysis is done after reviewing 26 papers. Using PSNR value, different image formats like JPEG, BMP and PNG's performance are analyzed. From the PSNR value, it is seen that BMP has good quality and capacity. JPEG provide high security. BMP is not resistance against attack. For small size application PNG is good for security. Hence to transfer data secretly, one need to choose proper steganography method and proper cover image format.

REFERENCES

[1] A. Sajid Ansari, M. Sajid Mohammadi, and M. Tanvir Parvez, "JPEG Image Steganography based on Coefficients Selection and Partition," *Int. J. Image, Graph. Signal Process.*, vol. 9, no. 6, pp. 14–22, 2017, doi: 10.5815/ijigsp.2017.06.02.

[2] H. Damghani, F. B. Mofrad, and L. Damghani, "Medical JPEG image steganography method according to the distortion reduction criterion based on an imperialist competitive algorithm," *IETImage Process.*, vol. 15, no. 3, pp. 705–714, 2021, doi: 10.1049/ipr2.12055.

[3] D. D. Shankar and A. S. Azhakath, "Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO," *Multimed. Tools Appl.*, 2020, doi: 10.1007/s11042-020-09820-7.

[4] V. Snasel, P. Kromer, J. Safarik, and J. Platos, "JPEG steganography with particle swarm optimization accelerated by AVX," *Concurr. Comput.* , vol. 32, no. 8, pp. 1–11, 2020, doi:10.1002/cpe.5448.

[5] L. K. Gupta, A. Singh, V. K. Yadav, and A. Srivastava, "Performance Analysis of Open PuffSteganography Tool Using Various Image Formats," *SSRN Electron. J.*, pp. 1–7, 2020, doi: 10.2139/ssrn.3550941.

[6] J. Wang, C. Yang, P. Wang, X. Song, and J. Lu, "Payload location for JPEG image steganography based on co-frequency sub-image filtering," *Int. J. Distrib. Sens. Networks*, vol. 16, no. 1, 2020, doi: 10.1177/1550147719899569.

[7] I. I. Araujo and H. Kazemian, "Improving Steganographic capacity using distributed steganography over BMP," *Multimed. Tools Appl.*, 2020, doi: 10.1007/s11042-020-09298-3.

[8] K. A. Darabkh, A. K. Al-Dhamari, and I. F. Jafar, "A new steganographic algorithm based on multi directional PVD and modified LSB," *Inf. Technol. Control*, vol. 46, no. 1, pp. 16–36, 2017,doi: 10.5755/j01.itc.46.1.15253.

[9] A. T. Suhail, "Hide a secret file in several bmp images using the circular secret key," *PervasiveHealth Pervasive Comput. Technol. Healthc.*, vol. 2, pp. 699–711, 2020, doi:10.4108/eai.28-6-2020.2298162.

[10] S. M. Hardi, M. Masitha, M. A. Budiman, and I. Jaya, "Hiding and Data Safety Techniques in Bmp Image with LSB and RPrime RSA Algorithm," *J. Phys. Conf. Ser.*, vol. 1566, no. 1, 2020, doi: 10.1088/1742-6596/1566/1/012084.

[11] D. I. Magomedova and O. I. Sheluhin, "Fractal Models and Algorithms for Creating a Protective Marking for Integrity and Authenticity Bitmap Images," *2020 Syst. Signal Synchronization, Gener. Process. Telecommun. SYNCHROINFO 2020*, 2020, doi: 10.1109/SYNCHROINFO49631.2020.9166069.

[12] D. Darwis, N. B. Pamungkas, and Wamiliana, "Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness," *J. Phys. Conf. Ser.*, vol. 1751, no. 1, 2021, doi: 10.1088/1742-6596/1751/1/012039.

[13] S. Id, "Securing secret data using an enhanced blowfish encryption with Image Steganography using Pixel Indicator Technique Farrukh Hassan Abbas."

[14] A. S. Ansari, M. S. Mohammadi, and S. S. Ahmed, "Digital colour image steganography for PNG format and secured based on encoding and clustering," *Int. J. Eng. Res. Technol.*, vol. 13, no. 2, pp. 345–354, 2020, doi: 10.37624/ijert/13.2.2020.345-354.

[15] A. Gupta, "STEGONOGRAPHY WITH PNG IMAGE FORMAT : WEB SUPPORTINGMEDIA," vol. 7, no. 1, pp. 2348–2350, 2020.

[16] Z. Lu, Z. Yin, and B. Luo, "Multiple reconstruction compression framework based on PNGimage," *arXiv*, vol. 7, no. 1, pp. 1–12, 2019, doi: 10.5121/ijcsity.2019.7401.

[17] A. Srinivasan, J. Wu, and J. Shi, "Android-stego: A novel service provider imperceptible MMSsteganography technique robust to message loss," *MOBIMEDIA 2015 - 8th Int. Conf. Mob. Multimed. Commun.*, 2015, doi: 10.4108/icst.mobimedia.2015.259071.

[18] P. Rai, S. Gurung, and M. K. Ghose, "Analysis of Image Steganography Techniques: A Survey," *Int. J. Comput. Appl.*, vol. 114, no. 1, pp. 11–17, 2015, doi: 10.5120/19941-1731.

[19] N. Akhtar, S. Khan, and P. Johri, "An improved inverted LSB image steganography," *Proc. 2014 Int. Conf. Issues Challenges Intell. Comput. Tech. ICICT 2014*, pp. 749–755, 2014, doi: 10.1109/ICICICT.2014.6781374.

[20] U. A.J., P. R. Kamble, and A. V. Thakre, "Comparative Study of Edge Based Lsb Matching Steganography for Color Images," *ICTACT J. Image Video Process.*, vol. 06, no. 03, pp. 1185– 1191, 2016, doi: 10.21917/ijivp.2016.0173.

[21] Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," *2018 Int. Conf. Inf. Commun. Technol. ICOIACT 2018*, vol. 2018-Janua, pp. 191–195, 2018, doi: 10.1109/ICOIACT.2018.8350661.

[22] Rojali, A. G. Salman, and G. George, "Website-based PNG image steganography using the modified Vigenere Cipher, least significant bit, and dictionary based compression methods," *AIP Conf. Proc.*, vol. 1867, 2017, doi: 10.1063/1.4994462.

[23] Y. Chen, S. Chien, and H. Lin, "True Color Image Steganography Using Palette and MinimumSpanning Tree," pp. 273–278.

[24] A. Pradhan, K. R. Sekhar, and G. Swain, "Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks," *Secur. Commun. Networks*, vol. 2017, 2017, doi:10.1155/2017/1924618.

[25] P. Mathivanan and A. Balaji Ganesh, "ECG steganography based on tunable Q-factor wavelettransform and singular value decomposition," *Int. J. Imaging Syst. Technol.*, vol. 31, no. 1, pp. 270–287, 2021, doi: 10.1002/ima.22477.

[26] BMP Information http://www.digicamsoft.com/bmp/bmp.html