Table 1. Performance anlysis of SA & RS

Input Size	Statistical Analysis (SA)		RS Steganalysis	
	Time (Sec)	Accuracy (%)	Time (Sec)	Accuracy (%)
253 K	0.01	0.65	0.01	0.65
30 M	1.01	0.65	1.40	0.65
130 M	8.45	0.65	10.45	0.65
200 M	13.13	0.65	12.65	0.65
340 M	32.02	0.65	17.50	0.65
600 M	63.57	0.65	18.56	0.65
1.73 M	132.13	0.65	21.06	0.65
2.55 G	429.47	0.65	26.65	0.65

Table 2. Performance Anlysis of ESA

Input Size	Extended Statistical Analysis (ESA)	
	Time(Sec)	Accuracy (%)
253 KB	0.01	0.4
30 MB	1.11	0.4
130 MB	5.21	0.4
200 MB	9.32	0.4
340 MB	13.0	0.4
600 MB	63.57	0.4
2.55 GB	28.54	0.4

7. CONCLUSIONS

Analyzing Forensic Multimedia is a crucial in this digitalization world due to increasing of innovative attacks and threats day by day. Forensic crime rate has been increasing rapidly. To reduce these kinds of attacks, as a first phase, needs to create awareness about various cybercrimes and their exploitation possibilities to the users of applications. Later, by following approved innovative standards and compliances in the development also can reduce victim ratio. One more approach to minimize the attack rate is adaptation of advanced technology tools in the digital applications. These can useful for prediction of threat, detection of attack and retrieve/extract the effected data by the unauthorized persons. The developed application is easy to use and is a new approach for detection of effected Multimedia. Further work will carry out on Audios.

REFERENCES

[1] Debbar, F., Ayad, B. (2017). A new steganalysis method to detect information hiding in speech. 13th International Wireless communications and Mobile Computing Conference (IWCMC), IEEE. https://doi.org/10.1109/IWCMC.2017.7986570

[2] Lai, B.,Chang, L. (2006). Adaptive data hiding for images based on HAAR discrete wavelet transform. Lecture Notes in Computer Science, 4319: 1085-1093. https://doi.org/10.1007/11949534_109

[3] Ing, X., Huang, W., Zhang, M., Zhao, I. (2016). A topography structure used in audio steganography. IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), pp. 2134-2138. https://doi.org/10.1109/ICASSP.2016.7472054

[4] Cheddad, A., Condell, J., Curran, K., Kevitt, M.P. (2010). Digital image steganography: Survey and analyses of current methods. Signal Processing, 90(3). https://doi.org/10.1016/j.sigpro.2009.08.010

[5] Anusha, P., Medhane, S.P. (2017). Trapping of stego images on the basis of statistical evidences. International Journal of Advanced Research in Computer Science, 8(5): 2003-2006. https://doi.org/10.26483/ijarcs.v8i5.3681

[6] Thomas, P. (2013). Literature survey of various steganography. International Journal of Engineering Research & Technology (IJERT), 2(5). http://dx.doi.org/10.17577/IJERTV7IS02000

[7] Curran, K., Devitt, J.M. (2008). Image analysis for online dynamic steganography detection. Computer and Information Science, 1(3): 32-41. https://doi.org/10.5539/cis.v1n3p32

[8] Wang, R.Z., Su, C.H., (2006). Secret image sharing with smaller shadow images. Pattern Recognition Lett., 27(6): 55l–555. https://doi.org/10.1016/j.patrec.2005. 09. 021

[9] Chen, P., Lin, H., (2006). A DWT based approach for image steganography. International Journal of Applied Science and Engineering, 4(3): 275-290. https://doi.org/10.15439/2016F521

[10] Aljamea, M., Athar, T., Iliopoulos, C., Msamiruzzaman, (2017). Detection of hidden encrypted URL in image steganography. The Ninth International Conferences on Pervasive Patterns and Applications, Patterns, pp. 3-8. https://doi.org/10.1145/2896387.2896408

[11] Saxena, N. (2017). Steganography scheme against RS attack enriched with evolutionary programming (AGA) and OPAP. International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS), 3(9): 64-68.

[12] Swadhin, K., Chirag, (2017). Video steganography using encrypted payload for satellite communication. IEEE Conferences Aerospace Conference. https://doi.org/10.1109/AERO.2017.7943978

[13] Kasapbasi M.C., Elmasry, W. (2018). New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check. Journal of Indian academy of sciences, 43(68): 1-14. https://doi.org/10.1007/s1204

[14] Westfeld, A., Pfitzmann, A. (1999). Attacks on steganographic systems. Proceedings of Third International Workshop on Information Hiding, pp. 61-76. https://doi.org/10.1007/10719724_5

[15] Djebbar, F., Ayad, B., (2017). A new steganalysis method to detect information hiding in speech. IEEE International Wireless Communications and Mobile Computing Conference (IWCMC). https://doi.org/10.1109/IWCMC.2017.7986570