An optimised implementation of steganography with two level of security

Lokesh Vishwakarma[1], Shivam Khare[2]

[1]M. Tech. Scholar, Vindhya Institute of Technology and Science,Jabalpur, (M.P) [India]

lokesh0202@gmail.com

[2]Assistant Professor, Department of Electronic & Communication Engineering ,Vindhya Institute of Technology and Science,Jabalpur, (M.P) [india]

shivamkahre2008@gmail.com

Abstract: Steganography is a kind of security technique present days; the way and art of hiding the existence of a message between sender and dedicated recipient. Steganography has widely used to hide secret data in various types of files, may be audio, digital images or video. The three most defined parameters for audio or image steganography are imperceptibility, robustness and its payload[3]. Various applications have their specific requirements for the steganography approach used. This paper aims to give an new method of image cum audio steganography, its applications and techniques. Paper work is an presentation of Audio and Image Steganography for the some plaintext, paper work also uses three isolated key and three layer of data protection, the overall avalanche in plaintext is very high in present paper work.

Keywords: cryptography, steganography, Peak Signal to noise ratio (PSNR), cover image, Mean Square Error (MSE), stegno object

I. INTRODUCTION

Information hiding is a famous research area, which is use for the applications such as copyright protection for watermarking or digital media or steganography and also fingerprinting [3]. All these techniques of information hiding are very different.

- In watermarking method, the message has information like owner identification along with digital time stamp, which usually applied for protection of data[3].
- In Fingerprint technique, the owner of the original data set uses a serial number that specially identifies the real user for the data set. This adds to data information to makes it possible to look out any unauthorized use of the data set and the intended user[3].
- Steganography approach hide the message which to be secure within the host data set and make it an unrecognizable information.

In that application, data information is hidden within a host data set and is required to be reliably communicated to a receiver. The master data set is corrupted purposely, but the converting way, is designed to make data invisible to an informal analysis.

The steganography modal is shown on Figure-1. Message is the actual data that the user wishes to transmit for make it confidential. It may be plain text, edited text, some image, or anything that can be present as a bit stream like as a copyright mark, a communication document, or a serial number. This method use Password is known as *stenography-key*[2], an optional choice. It make sure that only receiving end user who holds the corresponding decoding key and only he will be able to detect the message from a *cover-object*[2]. The massage carrier with the securly embedded message is then called the *stenography-object*[2].

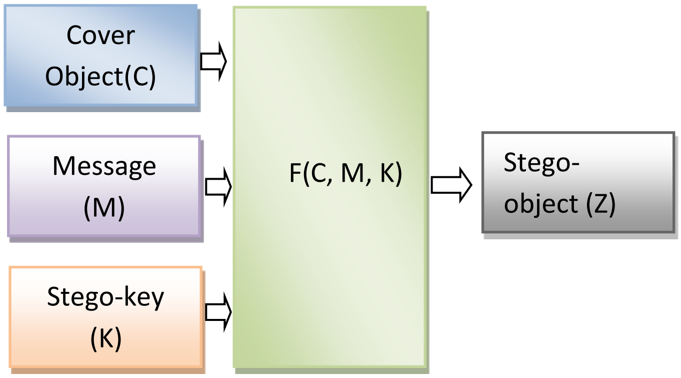

Figure 1 Basic Steganography Model

II. Objective

This paper work has the following objectives:

- To produce highly security tool based on cryptographic and steganography techniques.
- To describe techniques of hiding data using cryptography and steganography.
- To make a comparison of proposed work with available work
- To improve security level and to improve SNR of cipher and cover image

III. Problem statement

In steganography Network monitoring and surveillance systems will not flag messages and files that have steganography data[3]. So, if someone needs to steal hidden confidential data, they could conceal it within different file and send it in a simple looking email.Lots of data has to be transmitted which arises suspiciousness to the hackers and intruders[4].

IV. Methodology

Figure 2 shown below shows the methodology that we have adopted for the proposed work as can be seen the original data (D) is been divided into two parts D1 and D2, D1 and D2 are exact half of D.

D1 has been stenograph with the help of audio file for that number of sample (should be minimum 100 times of the characters in D2) and other length of key (range 100 to 255) has been provided as input parameters. For that recording wavrecord command is been used and the as the amplitude of voice is very low scaling is been done for providing appropriate amplitude so at the time of data hiding in voice file it cannot be interpreted. The mixing of data inside the audio file is substitution kind of change in voice sample at the step size decided by the key inserted.

D2 is been provided for image steganography and before actual providing it for hiding it in image its cipher is been generated with the help modulo multiplier where modulo of data is been taken as per the key provided in it, after generation cipher it gets transfer in binary for and as our cover image is been imported in MATLAB as in binary pixel form, first of all R, G and B components of cover image is been isolated so one can hide our binary cipher data in it. The method in proposed architecture is replaced LSB or 2nd LSB as in diagonal serpentine order. Also the decision of spacing between the hiding of cipher data bit is depends on the key that has been taken.

V. Results

Table 1 shown below are the results observed for proposed audio steganography as can be observe that Max value of SNR observed is around 82, and minimum mean square error is 0.0004 only.

Results observe for audio steganography			
Number of samples	**Size of data**	**SNR**	**MSE**
100000	2	76.8451	0.0014
110000	2	78.2550	0.0010
120000	2	81.8587	0.0004
130000	2	79.6327	0.0007

Table 1 : results of audio steganography

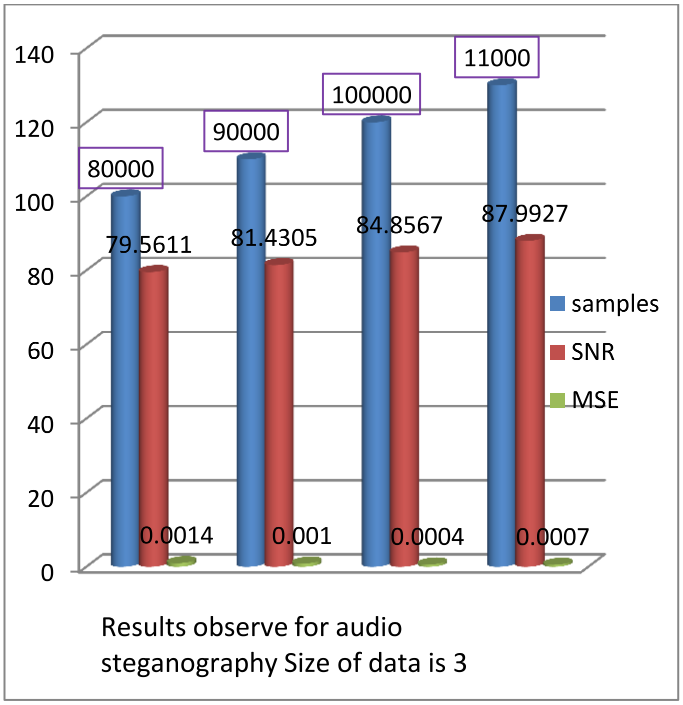

Figure 3: analytical results of audio steganography

Table 2 shown below are the results observed for proposed image steganography as can be observe that Max value of SNR observed is around 99, and minimum mean square error is 0.04888 only.

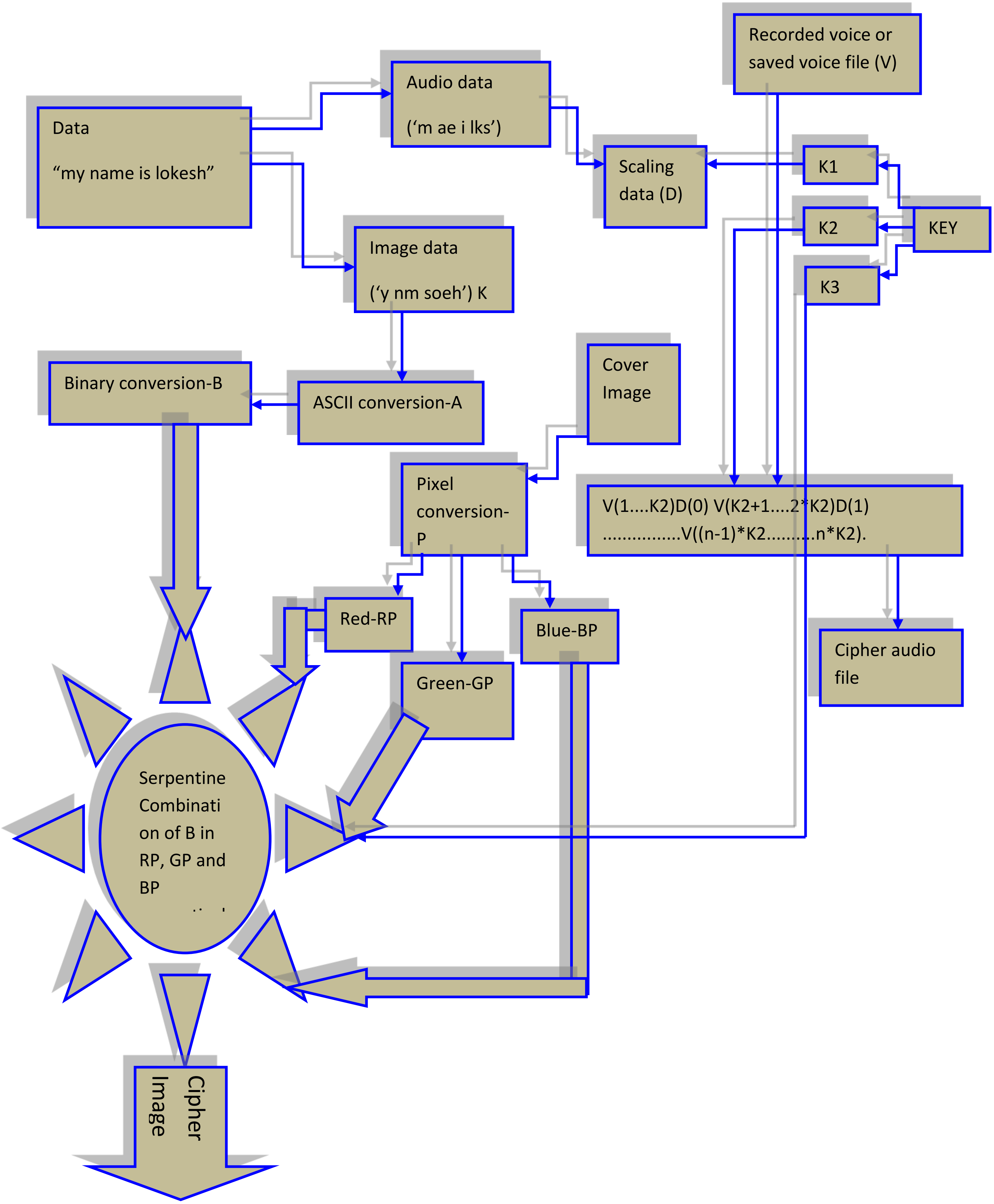

Figure 2: The proposed methodology

Results observe for image steganography			
Size of image	Size of data	SNR	MSE
2	151 kb	99.9599	0.0417
2	449 kb	99.0168	0.0684
2	278 kb	99.2781	0.0688
2	334 kb	97.1284	0.1270

Table 2: Image steganography results observed

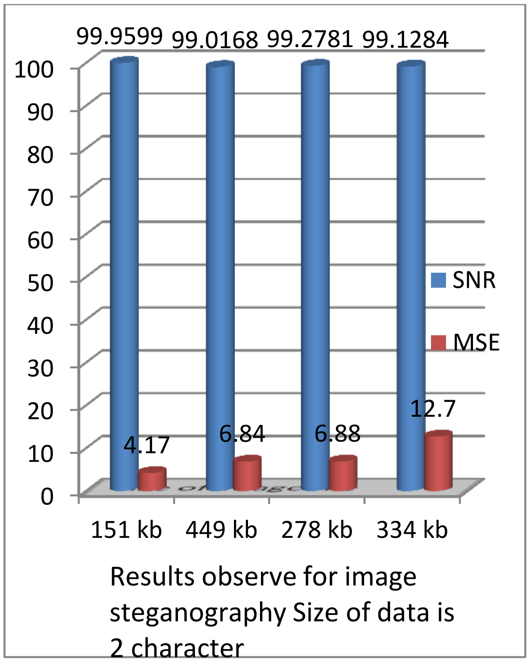

Figure 4: analytical results of image steganography

I. Conclusion and future scope

Both the cryptography and steganography have their own respective pros and cons, but the combination of both the model provides better protection of the data from the intruders. As can observed from the results the proposed method have less MSE and very good SNR value for both Audio and Image steganography. Proposed work has Increase in minimum value of SNR. Proposed work has Decrease in maximum value of SNR. Proposed work has decrease in standard deviation is approx. 82.5% as compare with base[1], and also less than any of available work.

In future the face recognition algorithms can be added to proposed method to improve the capacity of the steganography process without increasing any MSE[5]. In the case of cryptography, some more complex algorithms can be used then proposed work module, but the data usage, hardware implementation processing time and other factors should be taken into account [5].

References

1. Harish Kumar and Anuradha has published paper entile '**Enhanced LSB technique for audio Steganography**' in Third International Conference on IEEE, Computing Communication & Networking Technologies (ICCCNT), 2012.
2. Altaay and Alaa A. Jabbar and Shahrin Bin Sahib along with Mazdak Zamani has published paper entile, '**An Introduction to Image Steganography Techniques**', International Conference on IEEE, Advanced Computer Science Applications and Technologies (ACSAT), 2012.
3. V. Saravanan, A. Neeraja, has published paper entitle **Security Issues in Computer Networks and Stegnography,** 978-1-4673-4603-0/12, IEEE, Proceedings of7'h International Conference on Intelligent Systems and Control (ISCO 2013).
4. Marcelo E. Kaihara and Naofumi Takagi has published paper entile, "**A Hardware Algorithm for Modular Multiplication/Division**" , IEEE Transactions on computers, Vol. 54, No. 1, January 2005
5. Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath," **A secure and high capacity steganography technique**", Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013
6. Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, and Tai-hoon Kim," **Text Steganography: A Novel Approach**", International Journal of Advanced Science and Technology Vol. 3, February, 2009
7. Arvind Kumar, Km. Pooja , "**Steganography- A Data Hiding Technique**" , International Journal of Computer Applications Volume 9– No.7, November 2010
8. Neil F. Johnson, Sushil Jajodia , *"***Exploring Steganography: Seeing the Unseen***"*, IEEE,1998
9. MATLAB studies from Mathwork.com