Secured Biometric Signal Transfer using Steganography

Srinidhi G A [#1], K B ShivaKumar [*2]

[#] Research Scholar, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
[1] srinidhiga@ssit.edu.in
[*] Research Supervisor, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
[2] shivakumarkb@ssit.edu.in

***Abstract*— Biometric signals like images of Iris, figure print of the user, facial artifacts etc are being rapidly used in day to day activities today. With the implementation of the digital era, the idea of digital authentication for various purposes are in use for everyday activity. This paper presents a novel scheme for the purpose of securing the data which makes it possible for every user to secure the data and also to have a rightful authentication. The use of a digital technique called Hybrid steganography makes it possible to have a secured transaction between the communicating entities.**

Keyword - Steganography, Authentication, Secured Communication

I. INTRODUCTION

The advent of telecommunication services using internet has made it possible for each and every lay man to communicate not only the text but almost all types of data such as Text, Image, Audio, Video and many kinds of executable files also over an unsecured mode of transmission. The security of such files is of biggest concern of the day. There are many types of security mechanisms being employed to have a secured communication over the internet.

The first type of security being employed is cryptography. Cryptography is nothing but a securing technique in which the simple plain text (in case if it is in text format) will be considered which is simply encrypted into an unreadable format so that it will be not be read by the hacker. But the problem with this type of technique is that it makes it possible for the hacker that something fishy is being transmitted. This attracts his attention to try to decrypt it using one or the other way. In general, The process of cryptography doesn’t confine the very existence of the covert data.

The next usable digital technique is digital watermarking. Here, the logo or the authenticated information will be watermarked in such a way that it forms an authenticated copy of information. But yet again, this also will not conceal the very existence of the data.

Coming to steganography, this is a technique using which the very existence of the data itself is concealed so that people other than the intended users will not be able to even guess that there is a covert communication taking place. This paper is based on one such hybrid mode of steganography in which both cryptography and steganography are used to have a higher security for the data being transmitted. The results obtained are truly promising as it could have better results for different parameters like Peak Signal to noise Ratio (PSNR) Mean Square error (MSE) and capacity.

The paper has been organized in such a way that it gives a brief overview about the existing systems available in the literature. The model and the algorithm is discussed in section 3. The results of experimentation and discussions about it has been discussed in section 4. The paper concludes with conclusions and future scope.

II. EXISTING LITERATURE

Debnath Bhattacharyya et al.,[1] proposed a combined approach for steganography where the text is first encrypted using a key and then it is hidden behind a cover image. Even though many steganography techniques elaborates the same concept in several different way, the paper presents a good explanation of dependency of text and their ASCII as well as UTF values on the overall steganography and also introduces layer wise model.

Indradeep Banerjee et al., [2] presented text steganography method where encryption of the text is followed by hiding it in another text where characters are generated in an order such that they appear random to intruders. However authors have not emphasized on presenting a meaningful text as outcome of steganography which triggers suspicion. This technique could be more comprehensive if the text is hidden in cover text in such a way that resultant text is also correct text format.

Por and Delina [3] proposed a solution for the problem explained in [2] where text is hidden behind cover text such that result presents some meaning and are not just random sequences. However their statistical based approach needs huge cover text for hiding any text such that randomness of the characters is retained.

Shraddha et al., [4] came up with technique to hide the text message by dividing the letters into two groups of curvatures and non curvature letters. Further the text is hidden inside another text by encoding group ID followed by number of the letter in the group. This technique is quite unique. However it does not clearly elaborate the scenario as how curvatures are naturally identified by their algorithm. Also the technique depends upon the believe that the secret message is atleast a paragraph long. Dependency of the technique on length of the message and the paragraphs limits the technique.

Yousuf Bassil et al., [5] elaborated a technique to hide SQL queries by developing a meta dictionary to map different queries with different random selectively chosen table names and fields. Therefore this provides a good framework for generic text steganography where a method can be developed to append texts suitably into secret message such that not only the secret message can be retrieved at the receiver but at the same time schema of the text or domain of meaning of the text is retained.

Changder et al., [6] presented a novel steganographic technique to hide text using binary domain extraction. They first obtain the binary equivalent of the characters and hence sentences and then a similar sentence of character is obtained from an image that is closer to secret message. The technique still needs to supply a carrier image which makes the Steganography as more hybrid than pure text steganography. However their work on binary domain emphasizes on applying steganography on binary data rather than the text itself. This finding lays the foundation for our work where we use UTF data of the text to hide information. Indradip Banerjee et.al.,[7] proposed a procedure of text steganography using Indian Regional Language. Text steganography together with quantum approach based on the use of two specific characters and two special characters like invited comas (opening and closing) in Oriya language and mapping technique of quantum gate truth table was used to generate the stego text with minimum degradation. In this method the length of stego and cover remain same and this property enables the method to avoid the steganalysis also.

Christine K. Mulunda [8] proposed a genetic algorithm based model in Text Steganography worked with text as the cover medium with the aim of increasing robustness and capacity of hidden data. Elitism is used for the fitness function. The model presented is applied on text files, though the idea can also be used on other file types. M.Grace Vennice et.al.,[9] proposed a technique for hiding the Text Information using Stegnography using inter-word and inter paragraph spacing for hiding information. Shraddha Dulera et. al.,[10] proposed a method based on combining the random character sequence and feature coding methods to hide a character and evaluated the approaches based on metrics viz. hiding strength, time overhead and memory overhead entailed. it.

III. Proposed model

The figure 1 and 2 shows the overall block diagram of the model proposed in this paper. The detailed explanation of each stage of embedding is as given below.

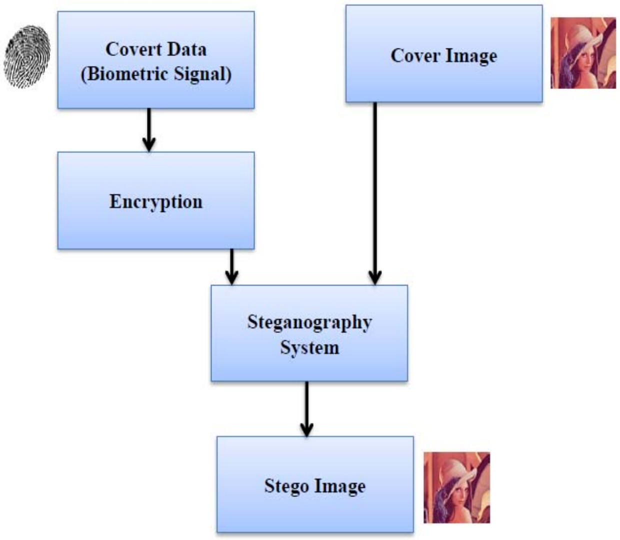


Fig 1: Embedding Algorithm

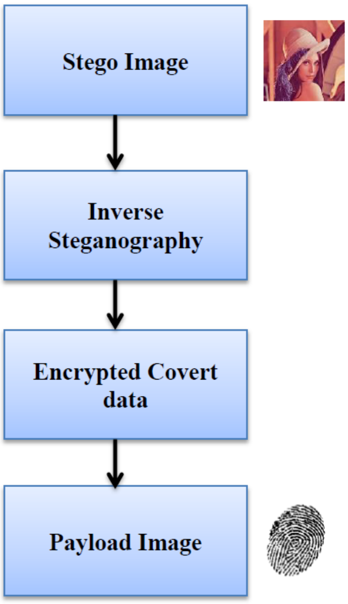


Figure 2: Extraction Algorithm

As shown in the figure the flow of the embedding process is as below:

a. Covert data: Here the covert data is nothing but the finger print of the user. In many of the applications, finger prints are used as an authentication data where in now a days, there are systems which uses remote authentication. Here, the required data is transmitted over the internet.

b. Encryption: The process here is very simple. The encryption process employed here is just the right shift of the bits of the pixel value. The trick used is based on the LSB bit of the pixel value. For example: if the LSB bit is 1, there will be 2 times right shift of the data. If the LSB bit is 0, then there will be one single right shift of the data. The output of this stage is the encrypted image which looks similar to the image before encryption. But the it's a known fact that, even a simple bit change makes the system to reject the digital finger print.

c. Cover Image: This is an image of any size and of any standard format like .tiff, .jpeg etc.

d. Steganography System: The simple LSB steganography method is used here for embedding of data but with a small change. Here, the data being used as a payload is the finger print which has to be extracted without even a single bit change. So unlike usual LSB steganography which embeds only higher nibble of each pixel, in this method, entire 8 bits of each pixel is considered and is embedded into the cover image.

e. Stego Image: The resultant of the embedding process taking place in steganography system is the stego image which apparently looks same as the cover data.

The extraction process is exactly the reverse process of embedding and is self-explanatory as per the flow.

IV. Experimental Results:

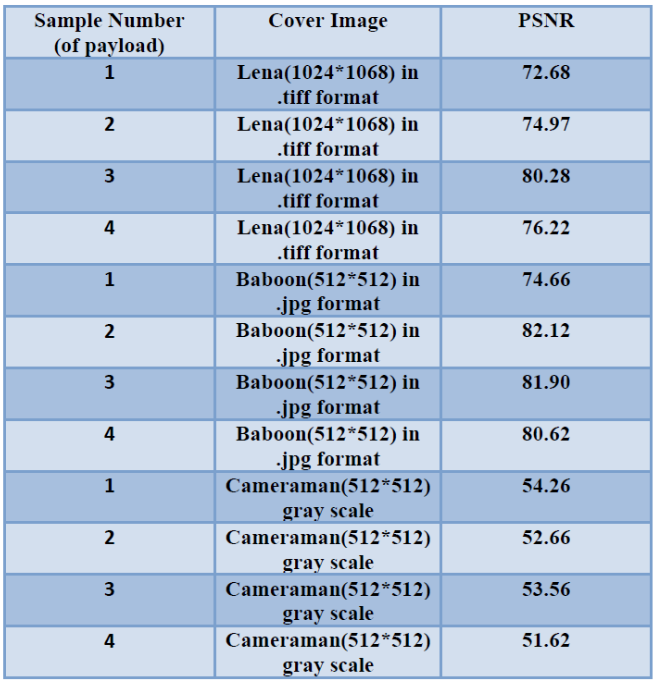
The algorithm was coded as a MATLAB code in which the data (both payload and cover) has been tested in different combinations. The payload which is the finger print of different users was tested by collecting the data from various users.

V. Discussions and conclusions:

As it is evident from the results as shown in table 1, the highest PSNR obtained is for the combination Baboon of resolution 512*512 which is in .jpg format and the finger print sample 2. It may be noted that as per the literature, PSNR above 40 is considered to be the working steganography system.[4,5,8]. But the system gives better PSNR which makes the system promising. The algorithm has also been tested with a grayscale image cameraman where the capacity of it will be less than the regular RGB image. Even then, the results are quite promising and are above the ones being discussed in the literature.

In future, the algorithm is planned to be implemented for other biometric signals like iris, ECG etc.

TABLE I EXPERIMENTAL RESULTS



Sample Number (of payload)	Cover Image	PSNR
1	Lena(1024*1068) in .tiff format	72.68
2	Lena(1024*1068) in .tiff format	74.97
3	Lena(1024*1068) in .tiff format	80.28
4	Lena(1024*1068) in .tiff format	76.22
1	Baboon(512*512) in .jpg format	74.66
2	Baboon(512*512) in .jpg format	82.12
3	Baboon(512*512) in .jpg format	81.90
4	Baboon(512*512) in .jpg format	80.62
1	Cameraman(512*512) gray scale	54.26
2	Cameraman(512*512) gray scale	52.66
3	Cameraman(512*512) gray scale	53.56
4	Cameraman(512*512) gray scale	51.62

REFERENCES

[1] Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, Tai-hoon Kim, “Text Steganography: A Novel Approach,” International Journal of Advanced Science and Technology,Vol. 3, February, 2009.

[2] 2. Indradip Banerjee, Souvik Bhattacharyya, Prof. Gautam Sanyal, “Novel Text Steganography through Special Code Generation,” International Conference on Systemics, Cybernetics and Informatics, pp 208-303, 2011.

[3] 3. L. Y. Por, B. Delina, “Information Hiding: A New Approach In Text Steganography,” International Conference on Applied Computer & Applied Computational Science, Hangzhou, China, 2008.

[4] 4. Shraddha Dulera, Devesh Jinwala and Aroop Dasgupta, “Experimenting With The Novel Approaches In Text Steganography,” International Journal Of Network Security & Its Applications, Vol.3, No.6, November 2011.

[5] 5. S.Changder, D. Ghosh, N. C. Debnath, “LCS based Text Steganography through Indian Languages,” International Conference on Computer Science and Information Technology, pp. 53-57, 2010.

[6] 6. Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal, “A Procedure of Text Steganography Using Indian Regional Language,” International Journal for Computer Network and Information Security, pp.65-73, 2012.

[7] 7. Christine K. Mulunda, Peter W. Wagacha and Alfayo O. Adede, “Genetic Algorithm Based Model in Text Steganography,” The African Journal of Information Systems, Vol 5, pp. 131-144, 2013.

[8] 8. M.Grace Vennice, Prof.TV.Rao, M.Swapna, and Prof.J.Sasi kiran, “Hiding the Text Information using Stegnography,” International Journal of Engineering Research and Applications, Vol. 2, Issue 1, pp.126-131, 2012.

[9] 9. Shraddha Dulera, Devesh Jinwala and Aroop Das gupta “Experimenting With The Novel Approaches in Text Steganography,” International Journal of Network Security & Its Applications, Vol.3, No.6, pp. 213-225, November 2011

AUTHOR PROFILE

Srinidhi G A received the BE degree in Telecommunication Engineering, from Visveswaraya Technological University, Belgaum, Karnataka, MTech degree in Sensor Systems Technology from VIT University Vellore, Tamilnadu, his Masters of Business Management degree from Sikkim Manipal University through Distance education. He has over 18 research publications in National and International conferences and journals. Currently he is working as Asst Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, image processing, Automotive Sensor systems, MEMS and Steganography

Dr K B Shiva Kumar received the BE degree in Electronics & Communication Engineering, ME degree in Electronics, MBA Degree from Bangalore University, Bangalore and M Phil Degree from Dravidian University Kuppam. He obtained Ph.D. in Information and Communication Technology from Fakir Mohan University, Balasore, Orissa. He has got 35 years of teaching experience and has over 60 research publications in National and International conferences and journals. Currently he is working as Professor and HOD, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, image processing, Multi rate systems and filter banks, and Steganography.