

**DEVELOPMENT AND DESIGNING OF AUDIO STEGANOGRAPHY WITH THE
HELP OF MULTILEVELED HASH-LSB AND RSA**

Anu,

*Assistant Professor (Resource Person), University Institute of Engineering and Technology
Mahrishi Dayanand University, Rohtak-124001, India
anukadyan01@gmail.com*

Abstract

In this era of rising technologies, transmission has become integral and important part of everyone's life as a result of its easier, quicker and safer use. The aim of this paper is to come back up with a method concealing the presence of secret message and increase the protection level. Steganography is that the craft of mystery correspondence. The point of it is to cover the nearness of correspondence. This paper utilizes the RSA Hash-LSB based Steganography, might be another develop for shrouded correspondence in present day propelled systems. It utilizes at least 2 steganographic procedures in a way that one innovation is a bearer for the second. Multi-Level Steganography has preferred standpoint of ominous cryptography and bringing about twofold assurance for the message. Here 2 very surprising steganographic procedures as Hash capacity and LSB are utilized instead of abuse one steganographic technique. This has been through with a particular determination of LSB's approach. This paper characterizes a system for sound steganography misuse Hash work, LSB change, and RSA encryption in multi-level steganography. This methodology provides a good manner of to realize higher security, to extend undetectability of high-ranking strategies, the clarity of digital audio signal mustn't be injured and to take care of the strength throughout the substitution of bits. We achieved a high PSNR and Low mean square error as compared to the previous studies to validate our results.

Index Terms – Encryption, Decryption, RSA, Hash, LSB

I. INTRODUCTION

CONFIDENTIALITY could be a crucial communication issue in various environments. In world, as an example, the main points of an enquiry are typically high secret, further as within the business world, wherever those details are associated with the event of a product. In step, a significant challenge in communication with info technology tools is expounded to info security. Specifically Security and privacy problems have long been investigated within the context of one organization sweat management over its users' access to resources [3]. Because of the issues inside the field of information security procedures like cryptography and steganography are utilized. In any case, use of cryptography infers the consideration of a mystery figure. Despite the fact that the figure won't not break anyway, it ought to in any case be achievable to catch it and to degenerate the message, making the information futile [4]. An integral way to deal with fight with this security question is to cover the key data amid an approach that clients aren't tuned into its reality,

i.e. as clients don't understand the information, the mystery is unbroken. This should be possible through steganography. Multi-Level Steganography could be another idea of information hiding in media transmission arranges that utilizations choices of Associate in Nursing existing steganographic system (the larger amount strategy) to frame a shiny new one (the lower-level technique). Multi-Level Steganography (MLS) was initially anticipated by Al-Najjar for picture steganography. MLS is predicated on joining 2 or a great deal of steganographic methodologies in such some way that one procedure (the upper-level) could be a transporter for the inverse strategy (the lower-level).

II. PROPOSED WORK

Our point is to plan a proficient plan that has a capacity to encode sound data. This work is centered around giving an answer for exchanging and sharing vital information with no bargain in security. All the presumed associations while sending business archives over the web dependably utilize encryption of the information to ensure spillage of data about their association to their adversaries or anybody. We have utilized multilevel security with hash-LSB and RSA to make a steganography calculation which is significantly more secure than numerous frameworks being utilized with the end goal of covertly sending information. In our examination we have actualized a sound steganography method utilizing Hash-LSB (Least Significant Bit) and alongside this to enhance security we are utilizing RSA calculation. For this we have begun with the encryption of the message into figure message by RSA calculation and afterward we are performing Hash-LSB to choose the particular areas in RGB slightest huge bits of a pixel.

III. EXPERIMENTATION

We exhibited a superior answer for encryption of sound in the system. Work begun with investigation of Steganography systems to discover procedures with better exactness and quality. Experimentation is begun with 1500×1150 reenactment range with 100 unit hubs with work in sender and collector correspondence under encryption mode. Basic parameters for simulation are given below in table 1.

Table1: Parameters used for experimentation

Name of parameter	Corresponding
Simulation tool	MATLAB
Time (simulation)	280 seconds
No of units	One Sender, One Receiver

Operation Mode	Encryption
Traffic Model	CBR

We processed with following encryption process from sender and receiver sides in network. Sender at ingress point started with covering the audio and along with secret message to follow for hiding as shown in figure 1. In our research first of all we have selected RGB audio as a cover audio. Then we have resized them to a standard sizes. The system contained an undisclosed message that was going to be embedded in the audio was identified.

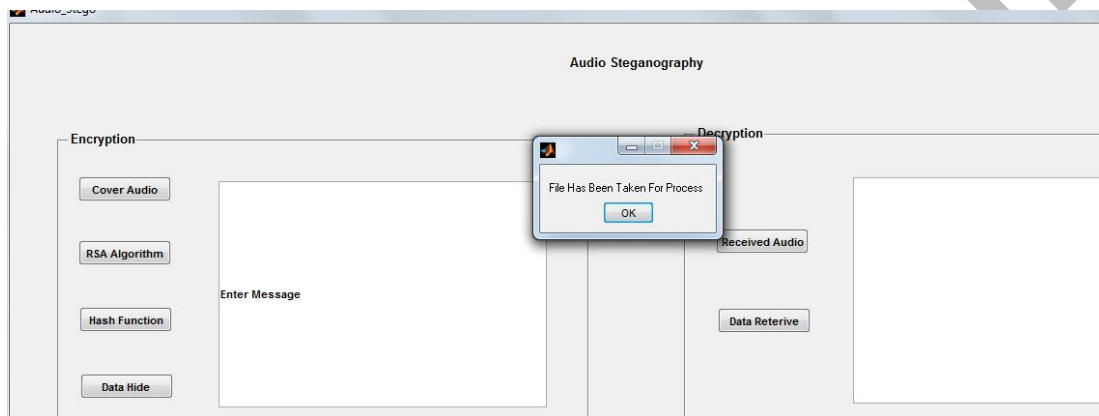


Figure 1: Encryption portal for our process

Hiding of information is basic requirement is fulfilled with encryption of message using RSA algorithm as shown in figure 2. This message is converted into ASCII values of the text alphabets, contained in the message. ASCII stands for the American standard code for information interchange which a character is encoding scheme based on the English alphabet. They represent text in computers. Then we have applied RSA algorithm, in we have taken two big prime numbers in start.

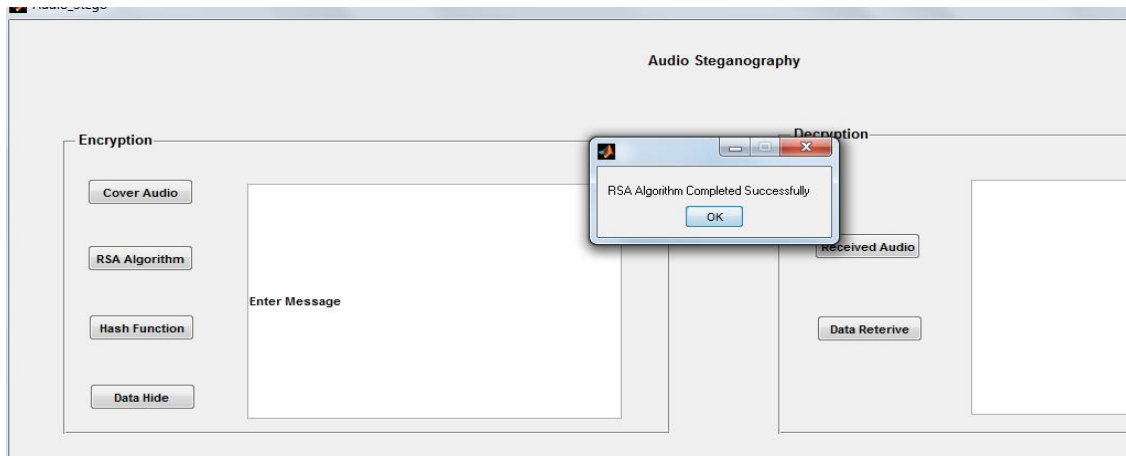


Figure 2: RSA Encryption for the encrypted method

Next process is to find Least Significant Bits from Cover audio for secret message hiding and after the application of function of the Hash Cover Audio LSB to attain the position. We have then embedded the encrypted message within LSB with multi levelled security and finally sending to the receiver. Receiver repeats the same steps at his side to extract the message using keys sent by sender.

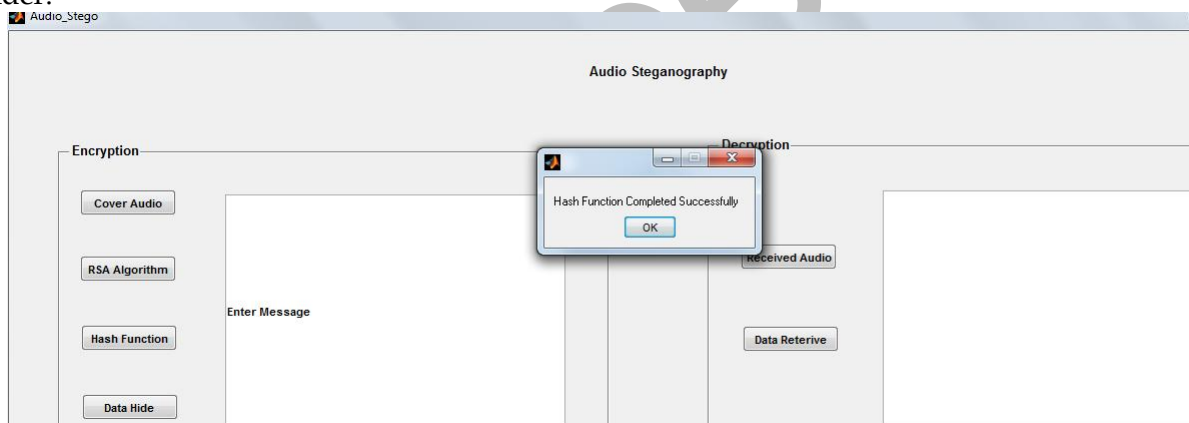


Figure 3: Hash LSB process

Toward the inception of this procedure we have taken figure message as the mystery message to be installed in the cover sound. In this procedure first we have changed over figure content into double frame to change over it into bits. At that point hash capacity is connected to sound which identified the slightest huge bits in RGB pixel esteems. At that point by utilizing hash work we have chosen the positions and after that 8 bits of message at once is taken and inserted in the request 3, 3, 2 in red green and blue segments individually. The procedure has proceeded till full message bits got installed in the cover sound.

In the decoding procedure we have again utilized hash capacity to recognize the position of the bits where the message bits are installed. At the point when the position of the bits is determined then the bits have removed from the position in an indistinguishable request from they were inserted. Toward the finish of this procedure we got message in twofold frame which was again changed over to decimal shape, and like this we have brought figure instant message as appeared

in figure 4.

The cipher text we got after the process of Hash-LSB is then taken as input in RSA decryption. By using public key generated in the key generation step of RSA encryption using decrypt function of RSA algorithm we have decrypted the cipher text into the ASCII values of the text. ASCII values are then easily converted back to their corresponding alphabets and in combination. We have got our text message taken at the start in a decrypted form.

We concluded the results in the form of message extracted and number of instructions which is also called as number of calls. It affects the process in a way that less is the number of calls, more is efficiency and more is the number of calls, less is the efficiency. Efficiency can be related to steganalysis. More efficiency means fewer chances of the steganalysis. In profile of our process we have specified the number of calls and time taken on particular process in between. Proposed work is shown through profiler in MATLAB and shown in figure 5 below.










Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
gcbf	7	0.005 s	0.005 s	
closereq	2	0.070 s	0.025 s	
genvarname>isCellString	2	0 s	0.000 s	
dect2hint	1	0 s	0.000 s	
...modemanager.uimodemanager>localDelete	1	0.005 s	0.005 s	
uitools.uimode.createuimode>localCleanUp	1	0 s	0.000 s	
...anager>@(obj_evd)(localDelete(hThis))	1	0.005 s	0.000 s	
genvarname>isString	1	0 s	0.000 s	
genvarname	1	0.040 s	0.010 s	
unique	1	0.025 s	0.015 s	
unique>uniqueR2012a	1	0.010 s	0.010 s	
intmax	1	0 s	0.000 s	
dec2hex	1	0.005 s	0.005 s	
iskeyword	1	0 s	0.000 s	
openfig>getToken	1	0.040 s	0.000 s	

Figure 5: Profiler view for proposed work

Number of directions is figured to characterize time multifaceted nature of a calculation. The time unpredictability of a calculation evaluates the measure of time taken by a calculation to keep running as a component of the length of the string speaking to the information. More are the quantity of guidelines more is the time intricacy. More is the time many-sided quality less is the proficiency. In our exploration we have chipped away at half and half mix of hash which takes 15 directions for process with RSA which takes approx 165 guidelines and LSB which utilize 8 bit for each set and approx 24 directions in blend. This blend assembles to be around 204 guidelines.

Table2: Comparison of PSNR value in previous work and our experimentation

	PSNR	MSE
Previous work	58.74	-----
Our process	169.94	0.00028

We calculated PSNR and MSE for our process and we found that our PSNR is greater than previous work considerably. Moreover in previous work MSE has not been mentioned and we found our MSE value to be very low that is 0.00028.

IV. CONCLUSION

In this work, discussion of the proposed work based on encryption based on audio encryption. Since we are using RSA and Hash with LSB algorithms for our process, the level of encryption is double and hence difficult to steganalyse. With it we are using an advanced version of LSB embedding technique i.e. hash LSB which has property of embedding the data in a way that there is least possibility of detection and steganalysis. In our proposed work, we applied same algorithms for audio processing with data hiding in stenography process and processed with 23 instruction set only which improved the results by approx 85 %. Figure 1, showing the detailed view of each instruction processed during the proposed algorithm working.

REFERENCES

- [1] Kamalpreet Kaur ,“ Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Encoding and Advanced LSB Technique”, International Journal of Security, Privacy and Trust Management, Vol. 1, No 2, April 2012
- [2] A. Swathi, “Video Steganography by LSB Substitution Using Different Polynomial Equations”, International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5, pp.1620, 2012.
- [3] P.Paulpandi, “Hiding Messages Using Motion Vector Technique in Video Steganography”, 2009 International Conference on Advances in Recent Technologies in Communication and Computing. Vol.34, Issue.1, 2009.
- [4] Vivek Sampat, “A Novel Video Steganography Technique using Dynamic Cover Generation”, National Conference on Advancement of Technologies - Information Systems & Computer Networks, Proceedings published in International Journal of Computer Applications, 2012.
- [5] Wikipedia [Online]. Available: <http://www.wikipedia.org/Steganography>.

- [6] Pritish Bhautmage," Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications, Vol.3, Issue.1, pp.1641-1644, January -February 2013.
- [7] MamtaJuneja, Parvinder Singh Sandhu," Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", IEEE International Conference on Advances in Recent Technologies in Communication and Computing, pp.33-39, 2009.
- [8] S. M. MasudKarim, Md. SaifurRahman, Md. Ismail Hossain," A New Approach for LSB Based Image Steganography using Secret Key", Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011) 22-24 December, 2011, Dhaka, Bangladesh
- [9] Hamdy M. Mousa," Secured Steganography Algorithm Based Random Function", IEEE Journal of Information Systems and Image Communication, Vol.3, Issue 1, pp.251-255, 2013.
- [10] G.A.V. Rama Chandra Rao, P.V. Lakshmi and N.Ravi Shankar," A Novel Modular Multiplication Algorithm and its Application to RSA Decryption",IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, pp. 251-260, November 2012.
- [11] RohitGarg, TarunGulati, "Security Analysis on Defenses against Sybil Attacks in Wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT), Vol.1, Issue.8, pp.1793-8236, October 2012.