Enhanced Audio LSB Steganography for Secure Communication

Muhammad Junaid Hussain
Rawalpindi/Islamabad, Pakistan

Khan Farhan Rafat
Islamabad, Pakistan

***Abstract*—The ease with which data can be remitted across the globe via Internet has made it an obvious (as medium) choice for on line data transmission and communication. This salient trait, however, is constraint with akin issues of privacy, veracity of the information being exchanged over it, and legitimacy of its sender together with its availability when needed. Although cryptography is being used to confront confidentiality concern yet for many is slightly limited in scope because of discernibility of encrypted information. Further, due to restrictions imposed on the use of cryptography by its citizens for personal doings, various Governments have also coxswained the research arena to explore another discipline of information hiding called steganography – whose sole purpose is to make the information being exchanged inaudible. This research is focused on evolution of model based secure LSB Steganographic scheme for digital audio wave file format to withstand passive attack by Warden Wendy.**

Keywords—Conceal; Human Auditory System (HAS); Imperceptible Communication; Internet as a Secure Communication Medium; LSB Based Audio Steganography; Modeling Security of Steganographic System; WAV File Steganography

I. INTRODUCTION

Steganography written as στεγανός γραφή means "Hidden/Covered/Concealed Writing", has its roots in Greek [1] and is not something new as it dates back to 440 B.C. [2]. Digital steganography came into glare of publicity when [3] reported its unlawful usage. 9/11 event indirectly contributed towards a serious drift of academics towards exploration of this field where a blend of encryption and steganographic techniques has emerged as a recommended solution [4] to achieve two fold security.

A. Terminology used in Steganography

Steganography works by selecting some carrier/container e.g., image, audio or video etc. called cover together with information to be hidden inside the cover referred to as message. The process of hiding is known as embedding and that of information retrieval is termed extraction reigned by a share secret called stego key between the communicating parties. The outcome of bit embedding is known as stego object while the entire activity at sending and receiving end constitutes a complete steganographic system [5].

B. Terminology used in Steganography

Steganography works by selecting some carrier/container e.g., image, audio or video files etc. [6] describes three types of steganography as follows:

- **Pure Key Steganography:** The oldest form of Stegaqnography employing schemes without any Stego key.
- **Secret/Symmetric Key Steganography:** The Stegnographic schemes make use of pre-agreed shared key that reign in the algorithm.
- **Public/Asymmetric Key Steganography:** It makes use of Public and Private Stego Key pair on the analogy of Asymmetric Cryptography.

C. Model

Simmon [7] was first to apprehend steganographic model widely known as 'Prisoner's Problem' where Alice and Bob held in imprisonment had to plan their scape on a pre-agreed protocol. Warden Wendy was there to monitor the message exchange between the two and could seize further communication in case of suspicion.

Type of constraints that Wendy may meet while examining communication between Alice and Bob include:

- **False Positive:** Wendy detects a cover with hidden message which in fact does not carry one.
- **False Negative:** Wendy lets go a cover that does carry a hidden message.

As ostensible, steganographic schemes must strive to force Wendy to commit 'False Negative' type of error.

D. Attacks on Steganographic System

Simmon [7] was first to apprehend steganographic model widely known Active and Passive type of attacks have been discussed in [8] where the former attempts to repeal the hidden information while the later is intended towards extracting the hidden contents without destroying original contents. However, [9] has discussed five type of attacks depicted in Fig. 1 followed by brief explanation of each.

- **Chosen Message attack**.This type of attack aims at analysing the stego object obtained from an input (message) of his / her desire i.e., to study the effect of embedding of known message on the cover.
- **Chosen Stego attack**.Here the attacker with known algorithm tries to extract hidden information from stego object of his/her choice.
- **Known Cover attack.**With original cover and the resultent stego object the attacker tries to contrast the

difference between the two to arrive at the hidden information.

- **Known Message attack.**Here the attacker tries to unfold the embedding algorithm while in possession of the actual message and the stego object.
- **Stego only attack.**The attacker tries to demystify the embedding algorithm inorder to extract hidden information by having the Stego Object alone.

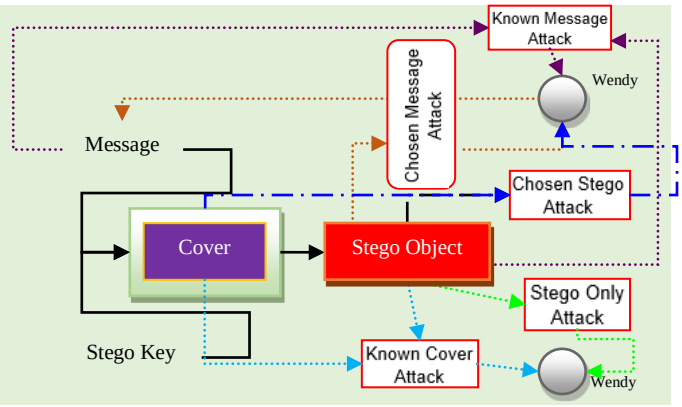

Fig. 1. Five Types of Attack on a Steganographic System

E. Perfect Security for Steganographic System

Kerckhoff's [10] opined that security of an algorithm in public domain resides in its key. In view of [1] "in a 'perfect' system, a normal cover should not be distinguishable from a stego-object, neither by a human nor by a computer looking for statistical patterns." Author in [11] discussed perfect security in context of following scenario: Amy creates a cover and embeds a random arrangement of secret message inside it under control of stego key. The stego object then reaches Bert through Crystal without suspicion. Bert may then retrieve the hidden message using the same (pre-agreed) stego key. Cachin [12] came up with equation (1) as a measure to estimate perfect security and asserted $\epsilon = 0$ as a requisite condition to achieve perfect security.

$$\varepsilon \leftarrow D(P_c||P_s) \leftarrow \sum_{q=Q} P_c(q) \log_2\left(\frac{P_c(q)}{P_s(q)}\right) \quad \dots\ \dots\ (1)$$

Pc & Ps signifies probability distribution of cover and stego object while Q is any finite set of alphabets.

[13] and [14] have already expounded at length on aforesaid discussion and in view of that we settle for imperceptibility and adherence to Kerckhoff's Principle as foremost bindings on any Steganographic scheme.

F. Audio Files and Formats

Pulse Code Modulation (PCM) is a technique for converting analog signals to digital format whose detailed discussion is beyond the scope of this paper, however, steps involved are depicted in Fig. 2 espoused from [15].

In general audio files are either flattened or uncompressed. Flattened audio may further be segregated into lossless (content preserving), and lossy that offers compact file size by persisting only prominent signals and includes MP3, AAC etc. as shown in Fig. 3. Uncompressed PCM is referenced by its sample rate (that confines the peak frequency relevant to specific file format) and bit-depth (a measure of noise within a signal). For example: Uncompressed CD audio takes 44,100 samples per second where each sample is banked as a 16-bit number. Uncompressed "WAV" file format is analogues to CD audio and is the focal file format for this exertion. For details on WAV file format [16] serves as a good reference.

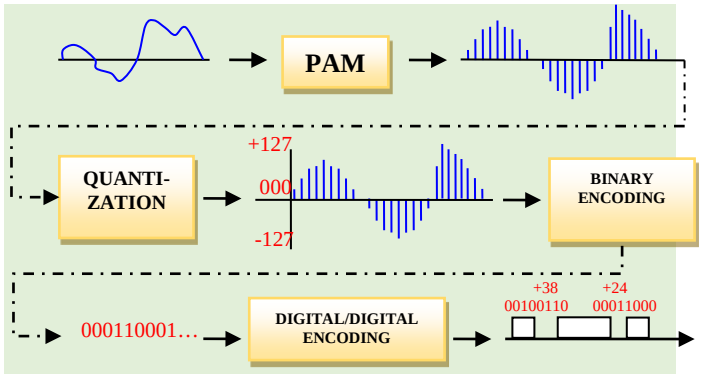

Fig. 2. Pulse Code Modulation (PCM). Analog-to-Digital Conversion

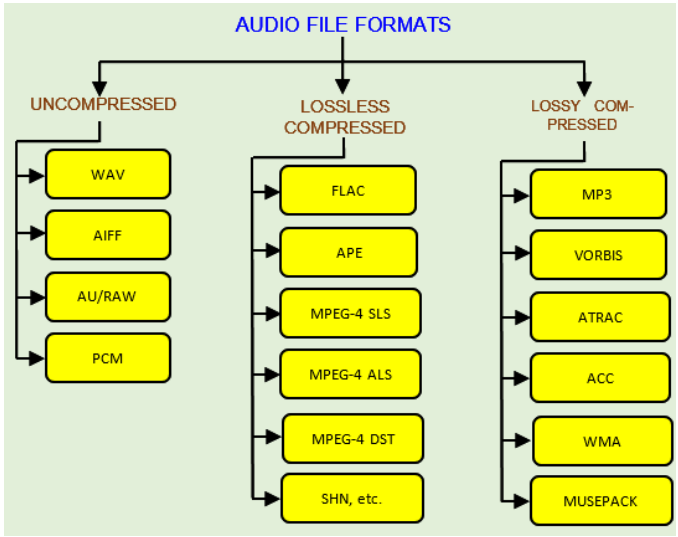

Fig. 3. Audio File Formats

By no means is audio steganography belittled in contrast to its counter parts like images and video etc. be-cause according to [17] "…the human auditory system (HAS) operates over a wide dynamic range. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than one thou-sand to one." This peculiar feature of HAS tends to undermine lower sound over louder ones and can be exploited either by acoustic or psychoacoustic models. Fig. 4 derived from [18] stretches a generalized view for data hiding inside audio files of which temporal domain (low-bit embedding) is the prima facie (prīmā faciē) of our research endeavor.

G. Evaluation Parameters

In [19] the impelling factors for audio quality includes (but are not limited only to) capacity of cover to hold secret data, and its imperceptibility of stego object in terms of Perceptual

Evaluation of Speech Quality (PESQ) computed vide equation (2) whereas robustness against deliberate amputation of hidden data remains undisputed perilous trait of any auditory steganographic system.

$$SNR_{db} = 10\log_{10}(\sigma^2_{signal} / \sigma^2_{noise}) \dots \dots (2)$$

where $\sigma^2_{signal} = \frac{1}{N}\sum_{i=1}^{N} Signal_i^2$ is the variance and is directly linked to noise power.

Lateral discussion in said reference include criteria specifically relating to active attacks (if) initiated by Warden Wendy mentioned below only for reference:

- Amplification
- Filtering
- Re-quantization
- Re-sampling
- Noise addition
- Encoding/Decoding
- Transcoding

H. Low-bit Encoding

The simplest and easiest way to hide information is the Least Significant Bit (LSB) embedding where message bit gets substituted in place of LSB of cover audio. The advantage lies in high embedding capacity whereas the disadvantage is its vulnerability towards noise insertion, amplification, and filtration according to [17].

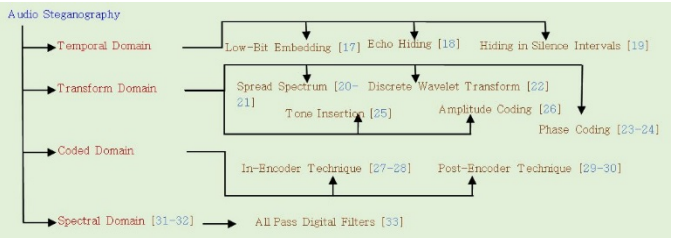

Fig. 4. Taxonomy of Data Hiding in Audio File

I. Paper Plot

Rest of the paper is organized as follows: Section II covers literature review of some of the most recent research on the subject followed by elaboration on our targeted LSB based steganographic scheme together with its limitations. Section III discusses modus operandi beginning with our statement of purpose followed by how we plan to achieve it (proposed logic/algorithm). Test results are shown in Section IV whereas Section V expound on theoretical aspect of proposed enhancement. Pros and cons come in Section VI. Section VII suggest future work while Section VIII concludes the discussion.

II. LITERATURE REVIEW

Following is a brief discussion on recent research focused on LSB steganography for audio files:

Authors in [20] have incorrectly stated SHA-1 as a PKE encryption algorithm. Their assertion "After receiving secret message's binary file salt and cover audio file salt; public key encryption algorithm i.e. SHA-1 is ap-plied to get the encrypted file. Finally, this encrypted data is hidden in cover audio." renders their proposed algorithm as nothing more than a fabricated piece of work. Authors in [21] have used the basic LSB technique to hide encrypted data without deliberating on the encryption algorithm used. In [22] authors made use of Modulus 16 for selecting target locations within audio file to embed four bit chunks of secret information. Au-thors in [23] have come up with two steganographic schemes. The first scheme "…instead of directly replacing LSBs of digitized samples with the message bits, it first checks the parity of the samples and then carries out data embedding." While the second flips/left un-changed the LSBs of the sample such that it's XOR with 2nd LSB points to secret message bit. [24] appears identical to earlier work of [25] in its approach towards hiding information inside audio carrier grounded on Genetic Algorithm based LSB embedding except that it first encrypts the message and then performs bit embedding in high order bits of targeted samples. The core idea is to select a random bit point in original audio sample, replace that bit with secret message bit and alter the remaining bits of the sample for close approximation with that of the original sample. Author in [26] which is also our targeted scheme for enhancement simply used two files and termed those as "two intermediates" to transmit the hidden secret thereby asserting on its security. The first of the two files is the stego object that carries hidden data at three LSB positions of sampled data ar-ranged in 2D mapping while the other conveys corresponding locations of the chunks carrying the hidden data via meaningful English sentences arrived at through the use of context free grammar (CFG). Noticeable limitations of targeted scheme include the following:

- Not in accordance with the definition of steganography.
- Not in accordance with Kerckhoff's Principle.
- For the system to operate correctly the stego object and the file holding coordinates corresponding to audio samples containing hidden information must be handy at any given time – i.e., in the absence of any of the two referred files the system may not be available for use. Further, there must also exist some logical connectivity between the two files or else will complicate the extraction process (in case of miss-matched files) that in turn poses a security risk.
- The contribution is silent over handling of repeated occurrences of same sequences (if any) of the randomly generated coordinates.
- By default, the cover need to be kept secret/destroyed and may not be reproduced/reused during the entire us-age of the system in order to preserve system's security.
- The information being exchanged defaults to "text message".

III. Modus Operandi

A. Statement of Purpose

To enhance security of LSB based audio file steganographic schemes using Wave file format.

B. Preliminaries

Confidentiality, integrity and availability (C.I.A.) of information merits security [27]. Cryptography is a preferred means to achieve confidentiality whereas Digital Signatures ensure integrity (of information) and non-repudiation (genuiness of sender). Availability, however, is linked with communication medium. To attain the said traits of Information Security we proceeded as follows:

- **Preferred Model:** As already stated we take inaudibility and adherence to Kerckhoff's principle as key traits to assure confidence in any audio related steganogaphic scheme, hence we have favored the model proposed by [28] which in turn is derived from [29] and [30] and is shown in Fig. 5. Our chosen model takes a preprocessed audio (cover) wave file and then performs key dependent varied (dynamic) 2-LSB bit embed-ding.

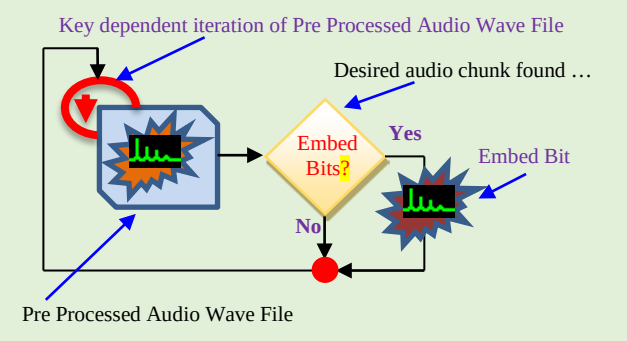

Fig. 5. Key Dependent Secret Bit Embedding

- **Message Header:** The noticible facet of our conducted literature review is that apart from [31] remaining schemes are silent on issue regarding length of hidden information which defaults to processing of entire audio file and then to construct actual message from that whch is extracted, though the logic used for its attainment is contentious and taken care of in our proposal. Further, all the schemes are silent over hidden data type which by convention seems to deafault as "textual information". Likewise, no concern shown towards integri-ty and non-repudiation of information being exchanged. Hence, to overcome the said impediments we constructed a twelve-byte header storing length of secert infromation, its type i.e., file extension, and its digital signature (three bytes for each) and appended it as a prefix to information being exchanged. Table 1 illus-trates this distribution for visual comprehension. The choice of HASH and Digital Signature algorithm has been left at user discretion. We, however, have opted for SHA-2, 256-bit HASH algorithm [32] (using 32 leftmost bits) and have used exclusive-Or encryption just for the sake of presenting our concept. Public key encryption algorithm RSA [33] is used to digitally sign message's HASH. Our proposed algorithm also make use of 256-bit Stego Key derived from [34] for test/experimental purposes.

TABLE I. Message Header with Scrambled and Hidden Audio Data

- 32 bits -	-- 32 bits --	---- 32 bits ----	---(8 x N) bits---
Length of Secret File	Secret File's Extension	Digital Signature **HASH**	Audio Data

- **Pre Processing of Audio (Cover) Wave File**: A True Random Number Generator (TRNG) whose details are beyond the scope of this paper is used to generate random bit patterns that replaces 2-bit LSBs of every 8/16-bit audio sample (chunk) of wave file.

C. Information Hiding

Bit embedding process is illustrated in Fig. 6, and is explained as follows:

Step 1: Iterate through every stego key byte and:
  i. Reduce stego key byte value to modulo 2 i.e., numbers in range 0, and 1 that corresponds to number of bits to be inserted at the time of secret bit embedding.
  ii. Store the result in sequence in a 32 byte array - say A1.
  iii. Add the two adjacent stego key bytes starting from index 1 and reduce the result to (modulo 2) + 1. Store the result in another 32 byte array - say B1in sequence. e.g., the adjacent byte for location B1 (31) will be B1 (0) and result will be computed as B1 (31) = (B1 (31) + B1 (0)) MOD 2 + 1.

Step 2: Select audio (cover) wave file.
Step 3: Preprocess selected cover.
Step 4: Select secret file.
Step 5: Calculate HASH of secret file.
Step 6: Encrypt the computed HASH value with sender's private key.
Step 7: Concatenate secret file's length, its extension along with encrypted HASH and affix it as pre-fix to selected audio wave file data.
Step 8: Perform exclusive-Or operation between the output of step 7 and stego key bytes. Stego key is iterated continuously till the referred output gets completely processed.
Step 9: Translate the outcome of Step 8 into bits which is the ready-to-embed secret information.
Step 10: For key dependent dynamic point to start bit embedding equation (3) is used, where denotes total number of 8/16-bit audio samples constituting the wave cover file.
Step 11: Iterate through preprocessed 8/16-bit audio samples starting from random position obtained vide Step 10 and proceed cyclically up to a point just before, by taking array A1 and B1 vide subsequent steps.

Step 12: Iterate array A1 (i) | i=0 to 31, one at a time.
Step 13: If A1(i) then take 'i' secret message bits and substitute these in place of one or two bits of 2-bit

LSBs of the selected sample starting at point indicated via B1(j) | j=i in cyclic order.

Step 14: Terminate bit embedding process when all secret message bits have been got processed other-wise proceed to Step 12.

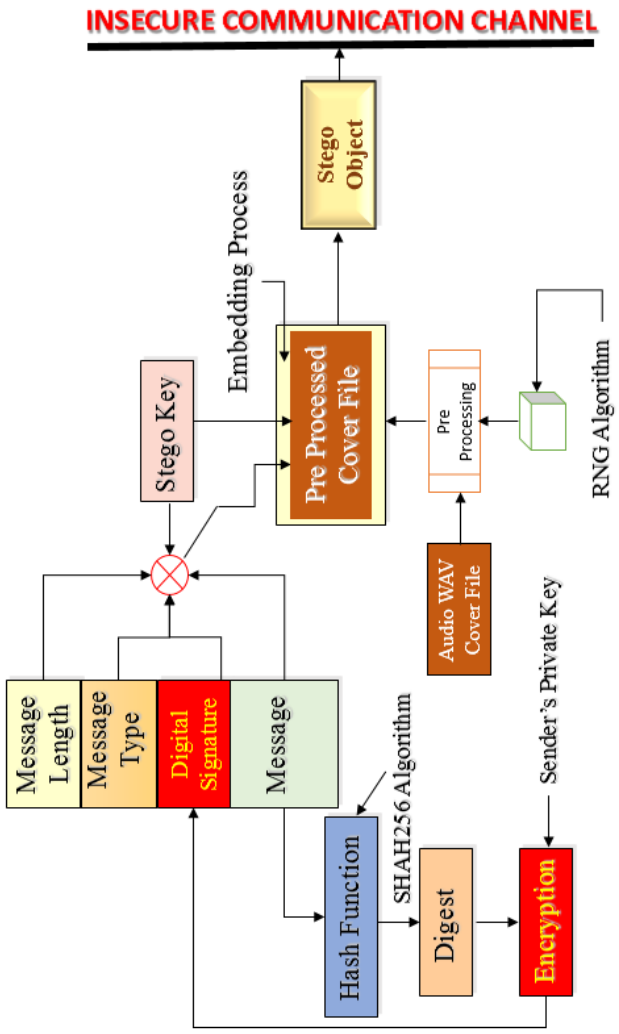

Fig. 6. Process of Bit Embedding

D. Information Extraction

Bit extraction process is shown in Fig. 7, and is explained as follows:

Step 1: Same as Section III - C (Step 1).
Step 2: Select audio (stego object) wave file.
Step 3: For key dependent dynamic point to start hidden bit extraction use equation (3).
Step 4 Iterate through 16-bit audio samples starting from random position obtained vide Step 3 ad proceed cyclically up to a point just before , by taking array A1 and B1 vide subsequent steps.

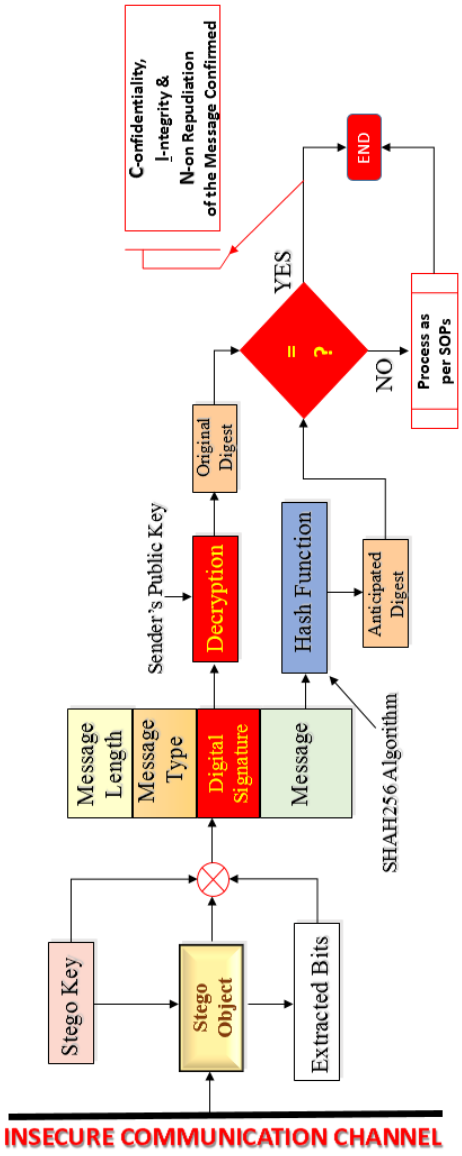

Fig. 7. Bit Extracton Process

Step 5 Iterate array A1 (i) | i=0 to 31, one at a time.
Step 6: If A1 (i) then extract and concatenate 'i' sample bits starting from point indicated via B1 (j) | j=i in cyclic order.
Step 7: If first ninety-six have been extracted from samples being processed then advance to Step 8 otherwise proceed to Steps 5.
Step 8: Perform exclusive-Or operation between the output of step 7 and stego key bytes. Stego key is iterated continuously till the referred output gets completely processed.
Step 9: Translate the outcome of Step 8 into bytes which is the hidden header whose first 32 bits holds the length of information being hidden, next 32 bits gives its extension while the remaining 32 bits gives the digital signature.

Step 10: Unfold the digital signature using sender's public key and store the output for lateral usage.
Step 11: Repeat Steps 6 and 7 till number of extracted bits equal to those contained in length of hidden message field of the header.
Step 12: Translate the outcome of Step 8 into bytes which is the hidden information.
Step 13: Calculate HASH of the hidden information.
Step 14: Compare the computed HASH with the value stored vide Step 10. If the two values are identical then the received information is authentic and has arrived from authorized sender. If, however, the two values contradict then laid down Standard Operating Procedures (SOPs) be followed.

IV. Test Results

Audio files (16 bit, single channel: 1, 10 kHz and 100, 250 and 440 Hz of 30 seconds duration each) that we experimented with, have been downloaded from [35].

In addition to Signal-to-Noise Ratio (SNR) computation (discussed earlier) following have also been contrasted for an in depth analysis of our proposed bit embedding methodology using [36]:

- Mean Square Error (MSE)
- Root Mean Square (RMS)
- Peak Signal-to-Noise Ratio (PSNR)
- Equivalent Quantize Bits
- Maximum Deviation
- Arithmetic Mean
- Signal-noise Correlation
- Noise Autocorrelation
- Amplification

Table 2, Table 3 and Table 4 contrasts differences between source and preprocessed, source and stego object, and preprocessed and stego object respectively that speaks high of our proposed logic where the results out-shine those discussed in literature review.

TABLE II. Contrasting Cover and Preprocessed Audio Files

Parameters	*1kHz*	*10kHz*	*100Hz*	*250Hz*	*440Hz*
PSNR Square (dB)	86.37	86.38	86.37	86.37	86.34
PSNR Sine (dB)	83.36	83.37	83.36	83.36	83.33
SNR (dB)	80.16	80.17	80.16	80.16	80.13
Quantize Bits	13.553	13.554	13.554	13.554	13.548
RMSE (2^16)	1.574	1.573	1.573	1.573	1.58
|Max| (2^16)	3	3	3	3	3
DC (2^16)	-0.0067	-0.0035	-0.0037	-0.005	0.0065
S/N Correlation	0.022294	0.023311	0.022879	0.022991	0.000227
Noise AC	0.014153	0.006709	0.002286	0.004856	0.012227
Amplification	1.000002	1.000002	1.000002	1.000002	1

TABLE III. Contrasting Cover and Stego Object Audio Files

Parameters	*1kHz*	*10kHz*	*100Hz*	*250Hz*	*440Hz*
PSNR Square (dB)	86.37	86.38	86.37	86.37	86.34
PSNR Sine (dB)	83.36	83.37	83.36	83.36	83.33
SNR (dB)	80.16	80.17	80.16	80.16	80.13
Quantize Bits	13.553	13.554	13.554	13.554	13.548
RMSE (2^16)	1.574	1.573	1.574	1.573	1.58
|Max| (2^16)	3	3	3	3	3
DC (2^16)	-0.0067	-0.0035	-0.0037	-0.005	0.0065
S/N Correlation	0.02229	0.023307	0.02288	0.02299	0.000227
Noise AC	0.014153	0.006712	0.002284	0.004857	0.012225
Amplification	1.000002	1.000002	1.000002	1.000002	1

TABLE IV. Contrasting Stego Object and Pre-Processed Audio Files

Parameters	*1kHz*	*10kHz*	*100Hz*	*250Hz*	*440Hz*
PSNR Square (dB)	131.52	131.19	132.03	131.52	129.54
PSNR Sine (dB)	128.51	128.18	129.02	128.51	126.53
SNR (dB)	125.31	124.98	125.82	125.31	123.33
Quantize Bits	21.053	20.998	21.137	21.053	20.723
RMSE (2^16)	0.009	0.009	0.008	0.009	0.011
|Max| (2^16)	3	3	3	3	3
DC (2^16)	0	0	0	0	0
S/N Correlation	-0.00072	-0.00062	0.000181	-0.00025	-0.00001
Noise AC	0	0	0	0	0
Amplification	1	1	1	1	1

V. Theoratical Substance

Let $A_1 = \{s_1, s_2, s_3, \ldots s_t\}$ be our cover audio file with '*t*' samples, $M = \{m_1, m_2, b_3, \ldots, m_i\}$ be the secret information of '*m*' number of bits, and $K = \{k_1, k_2, k_3, \ldots, k_n\}$ be the '*n*'-bit key that controls how $m_i \in M$ gets embedded in $s_t \in A_1$ and $C=\{c_1, c_2, c_3, \ldots, c_t\}$ is the outcome (Stego Object) of operations where, through extended Van Diagram shown in Fig. 8, we may perceive the process of bit embedding as follows:

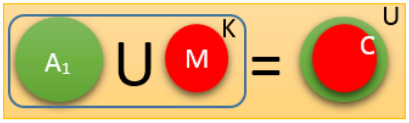

Fig. 8. Van Diagram Depicting Process of Bit Embedding

In principle A_1 Equals C only if outcome of encoding of *M* under control of *K* yields an exact pattern match as that of target bits of audio cover – Fig. 9 refers, chance of occurrences of which, however, are minimal. Hence, it is apparent from Fig. 10 that *for known cover and stego object the hidden information whether encrypted or plain can easily be arrived at by searching for unrelated patterns even without the knowledge of secret key*.

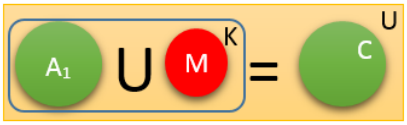

Fig. 9. Condition for Cover and Stego Object to remain Identical

Fig. 10. Extracting Hidden Information for Known Cover and Stego Object

The scenario for covert communication as perceived in [11] may be abridged as: For Alice and Bob to agree on their escape plan, Alice prepares a cover (*e.g., - a painting*) and sends it to Bob through Warden Wendy. Bob then alters the painting (*e.g., - enhance its coloring etc. based on pre-agreed secret parameter*) to implicitly convey details of escape plan and returns it to Alice that is more likely to get pass unnoticed by Wendy.

Foresaid above it is apparent that security of digital Steganographic system lies in deceiving Wendy to predict on actual cover used together with undetectable random diffusion of secret information inside its body, under control of some shared secret i.e., key, without the knowledge of which extraction of hidden information appear as hard-to-solve problem. Fig. 11 explicates on the concept (where preprocessed cover and extracted information are denoted by A_1' and M' respectively) to withstand Wendy's efforts in arriving at hidden information for a time sufficiently long enough where the significance associated with it loses its verve.

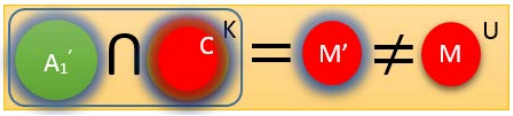

Fig. 11. Extrating Hidden Information from Preprocessed Cover and Stego Object

VI. Pros and Cons

Following are the advantages and limitation of our proposed improvisation:

A. Advantages

- Abiding definition of steganography.
- In accordance with Kerckhoff's Principle.
- Availability of original cover at the time of secret message bit extraction not required at recipient's end.
- Procedure for concealing secret message bit does not permit over writing of previously written/concealed data.
- The bit embedding procedure does not (not) necessitate to keep original cover secret/destroyed in order to preserve system's security.
- Ant File type can be hidden inside audio (WAV) cover.

VII. Future Work

We are in process of extending our research to 2 or more LSB bit manipulation to accomplish high data embedding capacity without compromising on security.

VIII. Conclusion

This paper presented a secure LSB based audio steganographic scheme through revelation of limitations in existing ones arrived at via literature review of recently published studies on the subject. The author has first laid theoretical foundation of the concept of secure steganography followed by logical affirmation using mod-el based scenario. A salient feature of the findings is that capacity of cover may not be attributed as an evaluation metric when it comes to evolution of secure steganographic scheme because the fewer the bits of secret information hidden in body of cover the more the chances are there for Wendy to commit false positive type of error and the more secure we are. An implicit trait of this research is to highlight the significance of Kerckhoff's Principle for steganographic systems whereas it has explicitly been shown that intelligence does not lie in embedding secret information in deeper sample layers of cover followed by alteration of its remaining bits but in inducing randomness (a technique which the Information Theory also endorse) during embedding process.

Reference

[1] Petitcolas, F.A.P.; Anderson, R.J.; Kuhn, M.G: "Information hiding: a survey." In: Proceedings of the IEEE, special issue on protection of multimedia content, vol. 87, issue 7, pp. 1062–1078 (1999).

[2] Stefan Katzenbeisser and Fabien A.P. Petitcolas, Introduction to information hiding. In Information Hiding: Techniques for Steganography and Digital Watermarking, Artech House. 1-14, Boston: 2000.

[3] Kelley, Jack. "Terror groups hide behind Web encryption." USA Today. 19 June 2001. URL: http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm (6 Nov 2001).

[4] Peter Wayner, "Disappearing cryptography: information hiding: steganography & watermarking", 3rd Edition, Morgan Kaufmann Publishers, 2009.

[5] RJ Anderson (ed.), Information hiding: 1st international workshop, volume 1174 of Lecture Notes in Computer Science, Isaac Newton Institute (Springer-Verlag, Berlin, Germany, 1996).

[6] Mohammed Salem Atoum, Osamah Abdulgader Al- Rababah, Alaa Ismat Al-Attili, New Technique for Hiding Data in Audio File. International Journal of Computer Science and Network Security (IJCSNS), Vol.11 No.4, pp. 173-177, April 2011.

[7] GJ Simmons, "The Prisoners' Problem and the Subliminal Channel", in Proceedings of CRYPTO '83, Plenum Press (1984), Pp. 51–67.

[8] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi. A Survey on Image Steganography and Steganalysis. Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, pp. 142-172, April 2011.

[9] A. Westfeld and A. Pfitzmann. Attacks on steganographic systems, in Proc. 3rd Int. Workshop on Information Hiding, vol. 1768, pp.61–76, 1999.

[10] A. Kerckhoffs, La cryptographie militaire, Journal des sciences militaires, 1883.

[11] Bret Dunbar, Steganographic Techniques and their use in an Open-Systems Environment, SANS Institute InfoSec Reading Room, 01/18/2002.

[12] Cachin, C., "An Information-Theoratic Model for Steganography," in Proceedings of the Second International Workshop on Information Hiding, vol. 1525 of Lecture Notes in Computer Science, pp. 306-31, Springer, 1998.

[13] Khan Farhan Rafat and M. Sher. "Innocuous Communication via HTML Document Hiding Data in Plain Sight", Arabian Journal for Science and Engineering (AJSE), September 2013. DOI: 10.1007/s13369-013-0685-z.

[14] Khan Farhan Rafat and M.sher. "On the Limits of Perfect Security for Steganographic System", International Journal of Computer Science Issues (IJCSI), Volume 10, Issue 4, No. 2, July 2013, pp. 121-126. www.ijcsi.org

[15] Behrouz A. Forouzan, Data Communications and Networking, 2nd Edition (Update), McGraw-Hill Company, 2000

[16] Wave File Format – The Sonic pot. http://www.sonicspot.com/guide/wavefiles.html

[17] Bender, W., et al., "Techniques for data hiding", IBM Systems Jour-nal, Vol. 35, Nos. 3&4, pp. 313-36, 1996.

[18] D Gruhl, W Bender, "Echo hiding", Proceeding of the 1st Inforomation Hiding Workshop, Lecture Notes in Computer Science, (Isaac New-ton Institute, England, 1996), Pp. 295–315.

[19] Bhagyashri A. Patil, Vrishali A. Chakkarwar, "Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 9, Issue 1 (Jan. - Feb. 2013), PP 30-34, e-ISSN: 2278-0661, p-ISSN: 2278-8727. www.iosrjournals.org

[20] Prof. R. Venkateswaran, Dr. V. Sundaram, Director, Implementation of ISS - IHAS (Information Security System – Information Hiding in Audio Signal) model with reference to proposed e-cipher Method, International Journal of Advanced Computer Science and Applica-tions (IJACSA), Vol. 2, No. 6, Pp. 112-116, 2011.

[21] Souvik Bhattacharyya, Arko Kundu, Gautam Sanyal, "A Novel Audio Steganography Technique by M16MA", International Journal of Computer Applications (0975–8887) Volume 30 – No.8, September 2011.

[22] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, "Information Hiding in Audio Signals", International Journal of Computer Applications (0975–8887), Volume7 – No.9, Pp. 14-19, Octo-ber 2010.

[23] Juhi Saurabh, Asha Ambhaikar,Audio Steganography using RPrime RSA and GA Based LSB Algorithm to Enhance Security, Internation-al Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

[24] Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, A Secure Audio Steganography Approach, Institute of Electrical and Electronics Engineers, 2009.

[25] Youssef Bassil, "A Two Intermediates Audio Steganography Technique, Journal of Emerging Trends in Computing and Information Sciences (CIS)", ISSN: 2079-8407, Vol. 3, No.11, November 2012.

[26] http://www.cisjournal.org/journalofcomputing/archive/vol3no11/vol3no11_3.pdf.

[27] Shon Harris, CISSP All-in-One Exam Guide, 6th Edition, McGraw-Hill Osborne Media, ISBN-10: 0071781749, ISBN-13: 978-0071781749.

[28] Khan Farhan Rafat and M. Sher, "Novel Perspective for XML Steganography, Accepted and under publication in International Journal of Networks and Security (IJNS)", Published by Recent Research Publication.

[29] Popa, R., "An Analysis of Steganographic Techniques." The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, 1998.

[30] J.Z Llner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G.Wicke, G.Wolf. "Modeling the security of steganographic systems", Proc. 2nd Workshop on Information Hiding, pp. 345-355, LNCS 1525, Springer-Verlag, Portland, 1998.

[31] Djebbar et al., "Comparative Study of Digital Audio Steganography Techniques", EURASIP Journal on Audio, Speech, and Music Processing 2012, 012:25, Pp. 1-16, http://asmp.eurasipjournals.com/content/2012/1/25.

[32] T Hansen - 2006, US Secure Hash Algorithms (SHA and HMAC-SHA), http://tools.ietf.org/html/rfc4634.

[33] VBForums – Thread: Equivalent of RSACryptoServiceProvider in Visual Basic 6.0, http://www.vbforums.com/showthread.php?548083-Equivalent-of-RSACryptoServiceProvider-in-Visual-Basic-6-0.

[34] HotBits: Genuine Random Numbers - John Walker's Fourmilab, www.fourmilab.ch/hotbits

[35] Minitab Statistical Software - Minitab: https://www.minitab.com/products/minitab/

[36] Download Audio Tone Files. http://www.mediacollege.com/audio/tone/download/

[37] WavDiff – Home. http://asp.lionhost.ru/en/tools_wavdiff.html