Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **6**, November **2018**

Compressed Sensing for Security and Payload Enhancement in Digital Audio Steganography

Muhammad Zeeshan Muzaffar

Barani Institute of Information Technology (BIIT),
PMAS-AA University, Rawalpindi, Punjab, Pakistan
Email: zeeshan@biit.edu.pk

Ijaz Mansoor Qureshi

Department of Electrical Engineering,
Air University, Islamabad, Pakistan
Email: imqureshi@mail.au.edu.pk

Atta-ur-Rahman*[,1], Fahd Abdulsalam Alhaidari[2], Mohammed Aftab Alam Khan[1]

College of Computer Science and Information Technology (CCSIT)
[1]Department of Computer Science (CS)
[2]Department of Computer Information System (CIS)
P.O. Box 1982, Dammam, KSA
Email: {aaurrahman,faalhaidari,mkhan}@iau.edu.sa
*Corresponding Author: aaurrahman@iau.edu.sa

Kiran Sultan

Department of CIT, JCC, King Abdulaziz University, Jeddah, KSA
Email: kkhan2@kau.edu.sa

Received February, 2018; Revised May, 2018

Abstract. *Digital Audio steganography is very popular research field nowadays comes with a lot of challenges like payload, security, imperceptibility and robustness. In this paper a novel technique for robust, secure and imperceptible digital audio steganography is proposed with heavy payload. We named this technique as Compressive Weighted Pattern Matching (CWPM) technique and it is used in combination with the Lifting Wavelet Transform (LWT). Use of compressed sensing (CS) provides the higher level of security and bigger payload by means of compression and encryption. Before CWPM, the cover audio is broken into segments, then LWT is taken for each segment till third level to maximize the embedding space. The detail subbands of first and second levels are used for data embedding while detail sub-band of third level is used to carry the encrypted indexes where data is being embedded. CWPM finds the position where data block can be embedded based on correlation. Experimental results show that the proposed technique not only provides a significant level of imperceptibility (more than 90% of NC) with excellent robustness. Simulation results show the validity and significance of proposed technique.*
Keywords: Compressive weighted pattern matching (CWPM), Compressed sensing (CS), Normalized correlation (NC), Audio steganography

1. **Introduction.** Cryptography, watermarking and steganography are technologies that are frequently being used to ensure the security, authentication and privacy (hiding) of data respectively, especially when it is transmitted over a public network according to [1-5].

In cryptography, the message is encrypted in such a way that it becomes incomprehensible. In watermarking, the message (watermark) is embedded in the host data (image/file) in such a way that host remains imperceptible and can be authenticated later, whereas in steganography the message is embedded in a cover signal without attracting attention [6-10]. Transmission of an encrypted message may create suspense for an eavesdropper, whereas this is not a case with a hidden message in a cover signal. Nevertheless, combination of these technologies can be used for a higher level of message protection [1]. Unlike cryptography, steganography and watermarking benefits from the perception limitations of human auditory and visual systems, which fail to recognize difference between host and watermarked/stego-signals respectively [11]. Usually, in steganography the media files such as, image, audio or video are used as host signals to hide the message data. In general, using an image or video as steganography cover signal is more popular than the audio. This is because Human Visual System (HVS) is far less sensitive to noise in the signal than Human Auditory System (HAS) [12-13]. The steganography algorithms need some features which depend on the transmission media and applications. The most important requirements are imperceptibility (transparency), robustness (security against certain attacks) and high embedding capacity [14-15]. Several digital audio steganography techniques have been proposed in the literature. Among them, least significant bit (LSB) based audio steganography technique is the first and foremost technique in which the data is embedded in LSB of the cover audio in time domain [12]. The LSB technique is the most imperceptible but least robust at the same time. Since in many attacks LSB of the signal is destroyed. Further to increase the robustness and embedding capacity, higher bits like 3^{rd} and 4^{th} LSBs have also been used but it was noted that the perceptual quality of the output signal is compromised [16]. Per [17], authors have employed five levels of packet integer lifting wavelet transform (ILWT) to decompose the cover audio into the sub-bands. After that, the hearing threshold is calculated for each sample in the ILWT domain per its sub-band. Based on the calculated threshold, data bits are embedded in the LSBs of the ILWT coefficients. Consequently, inverse ILWT is applied on the modified coefficients to construct the stego audio signal back in the time domain. In that study, an embedding capacity higher than 200Kbps with full data recovery has been achieved. In [18-19], authors have proposed a digital audio steganography technique, based on the ILWT. Moreover, 20% of the input speech signal embedding capacity was achieved with an acceptable ratio of transparency and successful recovery has been accomplished in that study. In [20-21], authors utilized compressive sensing in steganography. In another study, authors have adopted Wavelet Packet Transform (WPT) to decompose an audio cover signal to equal levels. After necessary scaling and converting the signal to binary, the LSBs of the details coefficients, which can be possibly used in the embedding process based on its strength, were selected. After that, the bits block matching between the LSBs of the host details coefficients and the message bits was performed in order to seek optimal positions for embedding the message bits. After that the altered coefficients were descaled and inverse WPT was performed to reconstruct the stego audio signal. In that study, authors have achieved a very high embedding capacity (about 300 kbps), with at least 50 dB signal to noise ratio (SNR) for the output perceptual quality. Although, this algorithm has a very high embedding capacity and excellent perceptual transparency, unfortunately its robustness is being compromised due to the multiplicative scaling. This type of scaling may cause losses in the recovered data [22]. To overcome the above cited problem same authors proposed a high capacity digital audio steganography scheme based on LWT and adaptive embedding positions [23]. In this technique, weighted block matching (WBM) was performed to find the suitable positions for data embedding. Eventually, the authors showed by the simulations that an embedding capacity of 300Kbps achieved

with a transparency of 35dB for the cover to noise ratio. Although the robustness was better than previous approach, still the scheme was not robust against certain attacks.

In this paper, we have employed compressed sensing (CS) for secret data transmission in conjunction with lifting wavelet transform. The secret message is compressed by CS prior to embedding. From CS two type of benefits are achieved namely payload compression and security enhancement that are shown by the computer simulations. Rest of the paper as follows: section 2 and 3 contain methodology and simulations while section 4 concludes the paper.

2. **Methodology.**

2.1. **Transmitter.** Let A=[a_1,a_2,...,a_b] be a cover audio of b samples and each sample having k bits. So, carrier signal has kb bits. f be the secret image of $n \times n$ to be transmitted. The following steps performed for each of the block (fig-1).

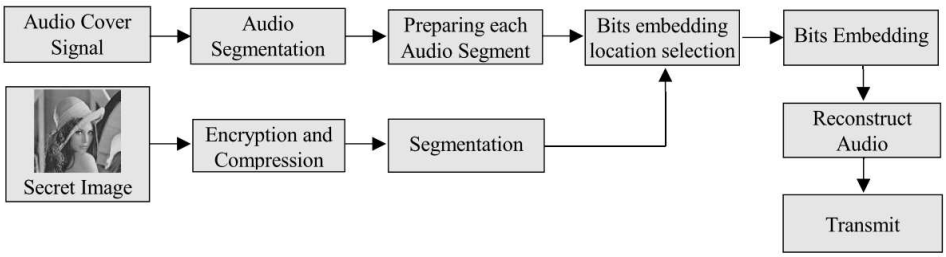

FIGURE 1. Secret message transmission

2.1.1. *Audio Segmentation.* Audio A contain b samples divided into G segments such that $b = Gq$, where q is the number of samples in each segment and in powers of 2. i.e A=[A_1,A_2,...,A_G] Where A_i=[a_{i1},a_{i2}...,a_{iq}] be the ith segment of cover audio A.

2.1.2. *Preparing Audio Segments.* Audio segment preparing involves third level of LWT so that the hidden message can be more imperceptible as shown in figure2. The outputs of preparing audio segment section are approximation and detail coefficients where $cA3_i$ and $cD3_i$ are third level approximation and detailed coefficients. $cD12_i$ is concatenation of first and second level detail coefficients vectors of ith segment A_i.

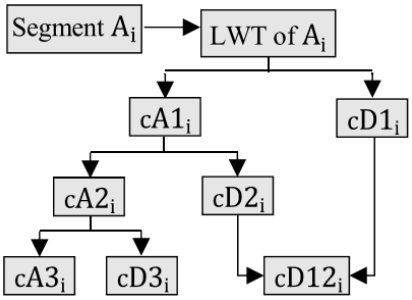

FIGURE 2. Preparing Audio Segments for Embedding

2.1.3. *Encryption and Compression of Secret image.* For sake of encryption and compression of our secret message, the concept of compressed sensing (CS) to be used here. The Shannon's sampling theorem states that to recover a signal, the sampling rate must be at least the Nyquist rate. Compressed sensing is based on the interesting fact that to recover a signal that is sparse in some domain representation, one can sample at the rate far below the Nyquist rate. This concept used here to decrease payload and enhance security as shown in figure3 mathematically.

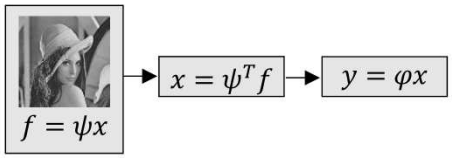

FIGURE 3. Encryption and compression of secret image

Here in figure3, f is an image having dimensions $n \times n$ containing n messages of $n \times 1$ each and ψ are the bases vectors matrix of the domain in which f can be sparsely represented with same dimensions as f. Coefficients of the new domain are represented by $x = \psi^T f$. Now, x is of $n \times n$ and φ which is sensing matrix having dimensions $m \times n$ where $m \ll n$. So, y which is our output of this module having dimensions $m \times n$. An important fact is that φ matrix is only known at transmitting and receiving side and hence introduce security and payload reduction.

2.1.4. *Segmentation.* This module includes the Segmentation of the encrypted message y having dimensions $m \times n$. As secret image is of r bit gray scale image. So, there are $r \times m \times n = s$ bits in total to embed. Secret message y segmented into g segments such that $s = gl$ where $0 < l \leq k$ be the length of each message segment. So, now after segmentation, the secret message will be of the form $y = [y_1, y_2, y_3, ..., y_g]$ Where each y_i segment is of l bits long. i.e.$y_i = y_{i1}y_{i2}...y_{il}$.

2.1.5. *Bits Embedding Location Selection and Bits Embedding.* Bits embedding location selection receives inputs from two modules which are "preparing audio segments" and "segmentation". First module outputs are $cA3_i$, $cD3_i$ and $cD12_i$ while second module output is y_i. Bits embedding location depends upon the maximum correlation between the ith $cD12_i$ and ith message segment y_i as shown in figure4. The following steps are followed to perform the functionality given in figure4.

- Map sign vector denoted by MSV_{12i} and MSV_{3i} formed to keep the signs of $cD12_i$ and $cD3_i$, respectively.
- Change all -ve values of $cD12_i$ and $cD3_i$ with their respective +ve values and convert it to binary.
- Now find the maximum correlation of message segment y_i and $cD12_i$ by using the following steps.
  - Find the first most significant bit of each coefficient of $cD12_i$ which is equal to binary 1 represented by $p_i = [p_{i1}, p_{i2}, ..., p_{ij}]$, where $i = 1, 2, ..., G$ and $j = 1, 2, ..., q/2 + q/4 = 3q/4$, where each p_{ij} represents the first MSB equal to 1 of jth coefficient of ith segment.
  - Now, two more factors are used to control the robustness against LSB attack and tolerance of change can be represented as L_{ij} and M_{ij} respectively. Where $L_{ij} < M_{ij} \leq p_{ij}$ and $p_{ij} - M_{ij} - L_{ij} \geq$size of y_i, if these condition does not meet in any coefficient of a segment $cD12_i$, then this coefficient will not consider for

correlation competition. Where L_{ij} points the location count from LSB of jth coefficient of ith segment and M_{ij} points the location difference from p_{ij} in the direction of LSB of ith coefficient of ith segment. i.e if $L_{ij} = 1$, $M_{ij} = 2$ and $p_{ij} = 7$, then the bits of jth coefficient of ith segment to find correlation can be seen in shaded area of figure below, so area from $5th$ location to $2nd$ location is the ROI (region of interest). A necessary condition is that ith message segment. M_{ij} points the $(p_{ij} - M_{ij})th = (7 - 2)th = 5th$ location.

- Find correlation of y_i with each ROI present in the coefficients of each segment of cover audio.
- Find the index with which the correlation of y_i is maximum.

After finding the maximum correlation index, replace the message segment y_i with that coefficients ROI present in $cD12_i$ and replace this index in $cD3_i$. Now modified detail coefficients becomes $\widehat{cD12_1}$ and $\widehat{cD3_1}$ respectively.

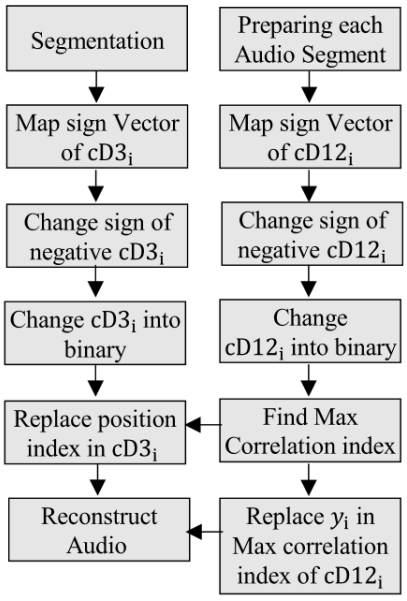

FIGURE 4. Bits Embedding location selection and Bits Embedding

2.1.6. *Reconstruct Audio.* After embedding secret message y_i, reconstruction of voice is performed. Approximate, modified detail and map sign vectors ($cA3_i, \widehat{cD12_1}, \widehat{cD3_1}, MSV_{12i}$ and MSV_{3i}) are the inputs of this module. To reconstruct the audio, first we must convert the binary values to equivalent decimals and place negative signs by the help of MSV_{12i} and MSV_{3i} and use inverse transform as shown in figure5.

2.2. **Receiver.** At receiver, to recover the secret message from the received audio S, first audio segmentation is performed. Size of segment should be the same as at transmitter. Received audio segments represented by S_t where $1 \leq t \leq G$. Now each S_t. Secondly, multilevel LWT performed uptill the level performed at transmitter which produces the $sA3_t$ (third level LWT approximate), $sD3_t$ (third level LWT details) and $sD12_t$(first and second level LWT details). After that, $sD3_t$ provide the indexes present in $sD12_t$ in which the y_t located. Then after getting all the $\hat{y}$'s, reassemble $\hat{y}$ having dimensions $m \times n$.

Now from these, we must estimate the $\hat{X}$ having dimensions $n \times n$ using following problem solving using CVX.

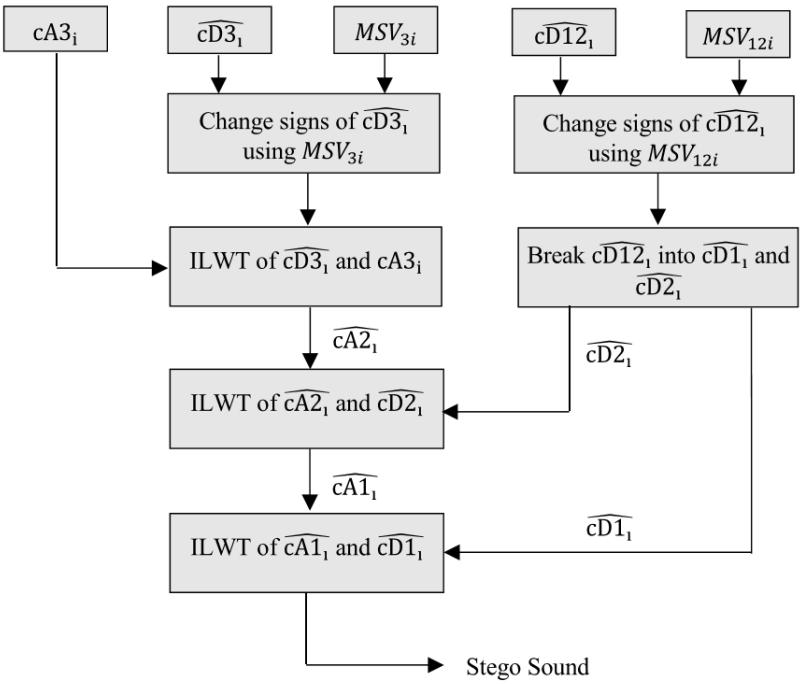

FIGURE 5. Audio Reconstruction

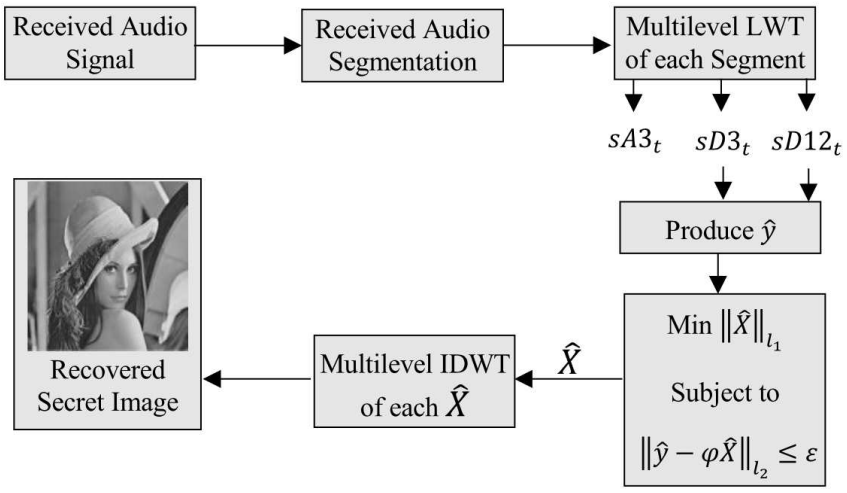

FIGURE 6. Reconstruction of secret message at Receiver

$$\text{Minimize } \| \hat{X} \|_{l_1}$$
$$\text{Subject to } \| \hat{y} - \varphi \hat{X} \|_{l_2} \leq \varepsilon$$

This $\hat{X}$ passes through the ILWT process and finally get the $\hat{f}$ having dimensions $n \times n$.

3. **Results and Discussion.** In this section, the authenticity of the proposed scheme is depicted through the MATLAB and CVX simulations in terms of robustness, transparency and payload etc. For the simulation, ψ is taken as multilevel two-dimensional Discrete wavelet transform and φ is the first m rows of QR decomposition of a Gaussian matrix of size $n \times n$ with $\{\pm 1\}$ as entries. So, φ is of $m \times n$. Nobody can recover estimate of y on receiver side without having φ. There are $2^{m \times n}$ possible φ's and it is near to impossible to check all of them. The possible huge number of φ's show the level of security achieved here

for different simulations shown in Table1. Table1 shows the level of security by showing the possible number of φ's. the minimum number seen in table1 is 1.6598×10^{181} which is a huge number for all possible combinations of φ's. This shows that our proposed scheme meets the security needs of steganography.

TABLE 1. Possible φ's for Security Enhancement

Figure	n	m	2^{n+m}
7b	512	250	5.9224×10^{225}
7c	512	200	2.1546×10^{214}
7d	512	150	1.9136×10^{199}
7e	512	120	1.7822×10^{190}
7f	512	90	1.6598×10^{181}
8b	512	150	1.9136×10^{199}
8c	512	120	1.7822×10^{190}
8d	512	100	1.6996×10^{184}
9b	512	150	1.9136×10^{199}
9c	512	120	1.7822×10^{190}
9d	512	100	1.6996×10^{184}

Figure 7(a) shows an original Lina image of dimension 512×512 in grayscale. After applying compressed sensing and embedding it into to cover audio, its recovered version is shown in figure 7(b) with compressed sensing parameters n=512 and m=250. Where m=250 means 104% increase in payload. The recovered image is very close to the original image in terms naked eye test. Further in figure 7(c) the compressed sensing parameter n is kept same while m is taken as 200. With m=200 means 156% increase in payload. In this way we are taking lesser information (more compressed and secure) for embedding in the cover audio. The result shows that the image is degraded compared to figure 7(b) but still it is perceptually acceptable. Similarly, in figure 7(d) the compression parameter m is taken as 150. With m=150 means 241% increase in payload. In figure 7(e) the compression parameter m=120 is taken very low. With m=120 payload increases to 326.67%. In figure 7(f) the m is taken extremely low as 90. With m=90 payload increases 468.88%. That means much secure and compressed but degraded compared to the former cases.

In figure 8 another example is shown. In figure 8(a) original sketch image is shown while in figure 8(b) and (c) its recovered images are depicted. In both cases the parameter m is taken as 150 and 120 and payload in both cases increases 241.33% and 326.66% respectively. The recovered images still considerably recognizable. On the other hand, in figure 8(d), for m=100, the payload increases 412% but edges of the images effect badly. This shows that as compression and payload increase, the quality of the recovered images decreases. Figure 9 presented another example of text-based images. Both uppercase and lowercase letters are used in this example and all possible letters of English used in the phrases. Figure 9(a) shows the original image of the text. In figure 9(b), (c) and (d), parameter m is taken as 150, 120 and 100 respectively. Figure 9(b) and (c) shows some degradations in quality of the images but are easily readable. But figure 9(d) shows degraded badly but still have the recognizable text. From these results, it is apparent that proposed scheme provides a good payload with significant level of and security.

Another achievement provided by compressed sensing is the compressibility ratio which also shows the payload enhancement per second and can be formulized as:

$$\text{Compressibility ratio} = \frac{number\ of\ bits\ in\ f}{number\ of\ bits\ in\ y}$$

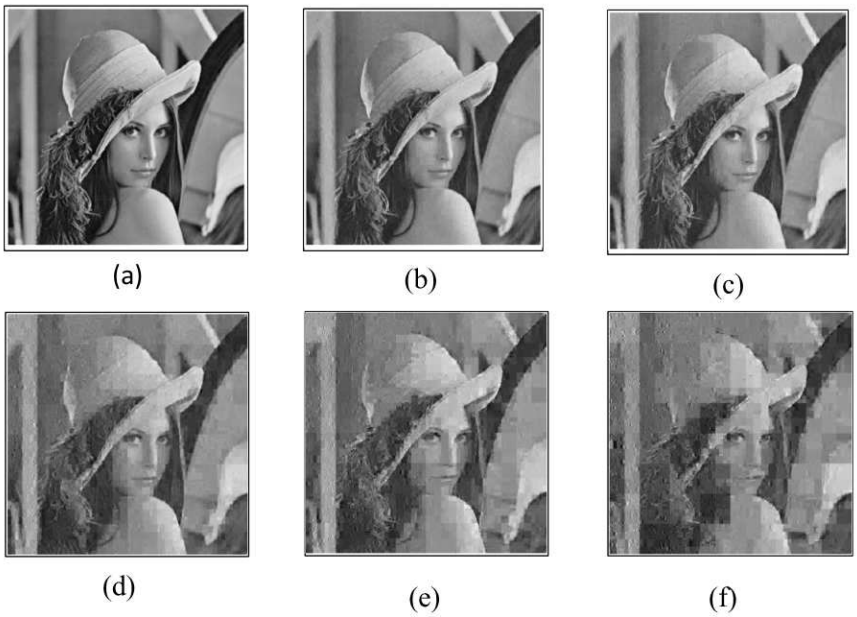

FIGURE 7. Recovery for (a) Original (b) n=512, m=250 (c) n=512, m=200 (d) n=512, m=150 (e) n=512, m=120 (f) n=512, m=90

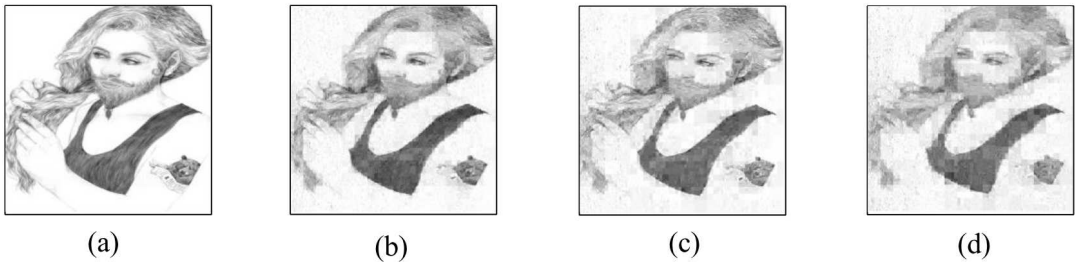

FIGURE 8. Secret Message Recovery (a) Original (b) for m=150 (c) for m=120 (d) for m=100

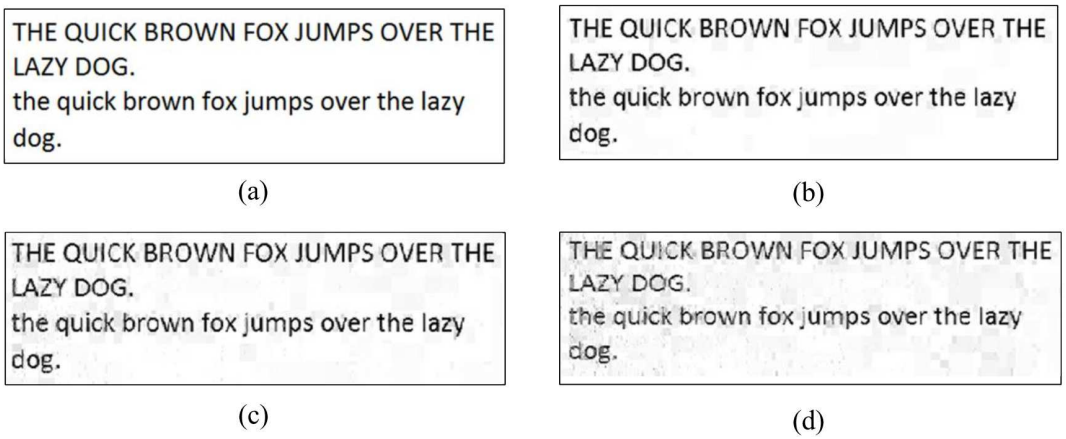

FIGURE 9. Secret Message Recovery (a) Original (b) for n=512, m=150 (c) for n=512, m=120 (d) for n=512, m=100

Where f be the original image and y is the image passes through CS process. Compressibility ratio for different images can be seen in Table2.

TABLE 2. Compressibility ratio

Figure	n	m	**Compressibility ratio**	**Figure**	n	m	**Compressibility ratio**
7b	512	250	2.048	Figure 8c	512	120	4.2666
7c	512	200	2.56	Figure 8d	512	100	5.12
7d	512	150	3.4133	Figure 9b	512	150	3.4133
7e	512	120	4.2666	Figure 9c	512	120	4.2666
7f	512	90	5.6888	Figure 9d	512	100	5.12
8b	512	150	3.4133				

For the sake of robustness test, normalized correlation (NC) is used as a figure of merit. NC used to test the level of correlation between the original and stego audio. Its value varies between 0 and 1. Formula for NC is

$$\text{Normalized Correlation} = \frac{\sum_{i=1}^{L} A_i S_i}{\sqrt{\sum_{i=1}^{L} A_i^2 \sum_{i=1}^{L} S_i^2}}$$

Where L is total number of samples in audio signal. A and S are original cover signal and the received stego signal respectively. Figure 10 shows the level of NC and shows the proposed scheme is highly robust against AWGN. The stego signal is tested at different levels of AWGN but the NC approaches to 1 at -25dBs for all kind of audio cover signals. Different types of voices are investigated including human voices (male, female) from different age groups and some natural sounds. It is worth mentioning here that the robustness of scheme is even higher in the case of human voices where the NC tappers off to 1 at -50dBs. That means the proposed scheme is quite useful for day to day human communication. In contrast to the scheme proposed in [16], where users demonstrated that their scheme is robust at 35dB and higher, our scheme saves 60dBs for natural sounds while 85dBs for human voices.

The difference between the spectrograms of original cover audio signal and the stego signal shown in figure 11 and figure12. Analysis shows that there is negligible amount of changes between the original and stego signal in the case of different female voices. This shows that the proposed scheme does not introduce much changes in their spectrograms. It is apparent from the figures that female voices spectra have better performance compared to male voices. This is perhaps because the female voices exhibit higher pitch compared to male voices. So, the frequency components are crisper and confined in female cases compared to male voices. Hence their spectra are less vulnerable to the changes offered because of the proposed scheme. Since in the proposed scheme the data is embedded in detail components of LWT.

Figure 13 shows the time domain changes in cover audio before and after embedding the secret message. In this regard, six examples are taken to analyse the time domain changes in the host audio due to our proposed scheme and all the examples shows that no significant change can be seen in the signals before and after embedding in time domain.

4. **Conclusion.** In this paper a novel digital audio steganography technique using compressed sensing with Lifting wavelet transform is proposed. In this technique, the compressed sensing is applied to the message image prior to embedding in the cover audio by means of LWT. Here, compressed sensing provides high level security because sensing matrix $\varphi(m \times n)$ is only known at transmitter and receiver and to estimate the real φ among

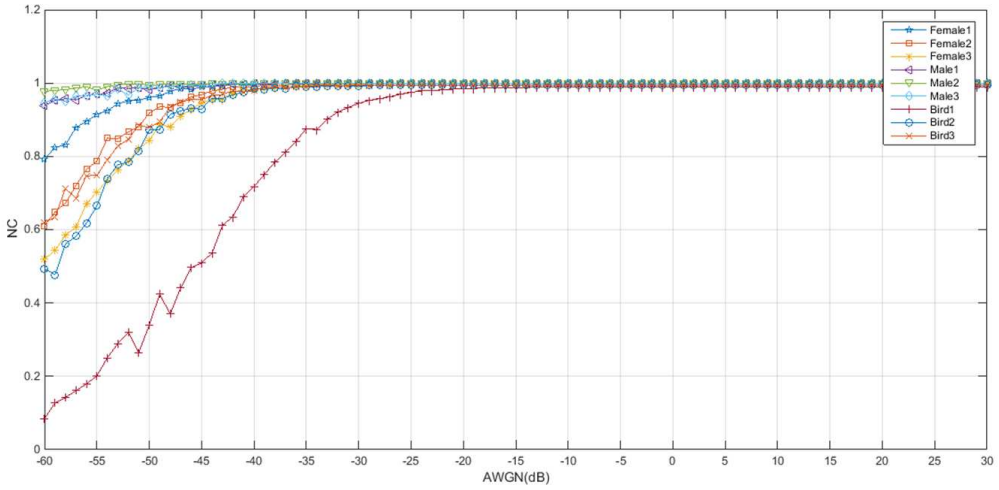

FIGURE 10. Normalized Correlation Vs NC

the huge number of φ combinations ($2^{m\times n}$) is nearly impossible. The simulation results show that the proposed scheme promises a great enhancement in payload, robustness, security and imperceptibility.

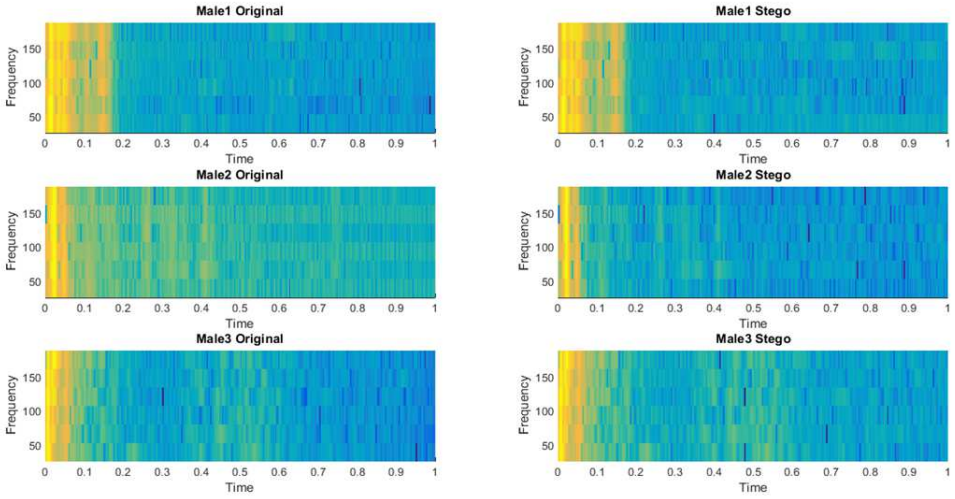

FIGURE 11. Spectrogram analysis of three male voices

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, & P. Kevitt, Digital image steganography: Survey and analysis of current methods, *Signal processing*, vol. 90, no. 3, pp. 727-752, 2010.

[2] A. Nissar, & A. H. Mir, Classification of steganalysis techniques: A study, *Digital Signal Processing*, vol. 20, no. 6, pp. 1758-1770, 2010.

[3] M. T. Naseem, I. M. Qureshi, Atta-ur-Rahman & M. Z. Muzaffar, Novel technique for capacity maximizing in digital watermarking using fuzzy rule base, *Journal of Intelligent & Fuzzy Systems*, vol. 27, no. 5, pp. 2497-2509, 2014.

[4] M. T. Naseem, I. M. Qureshi, T. A. Cheema, & Atta-ur-Rahman, Hash based medical image authentication and recovery using chaos and residue number system, *Journal of Basic & Applied Scientific Research*, vol. 3, no. 6, pp. 488-495, 2013.

[5] M. Z.Muzaffar, I. M. Qureshi , Atta-ur-Rahman, M. T. Naseem, Changing slope method: A novel technique for digital audio steganography, *J. Basic Appl. Sci. Res.*, vol. 3, no. 12, pp. 71-81, 2013.

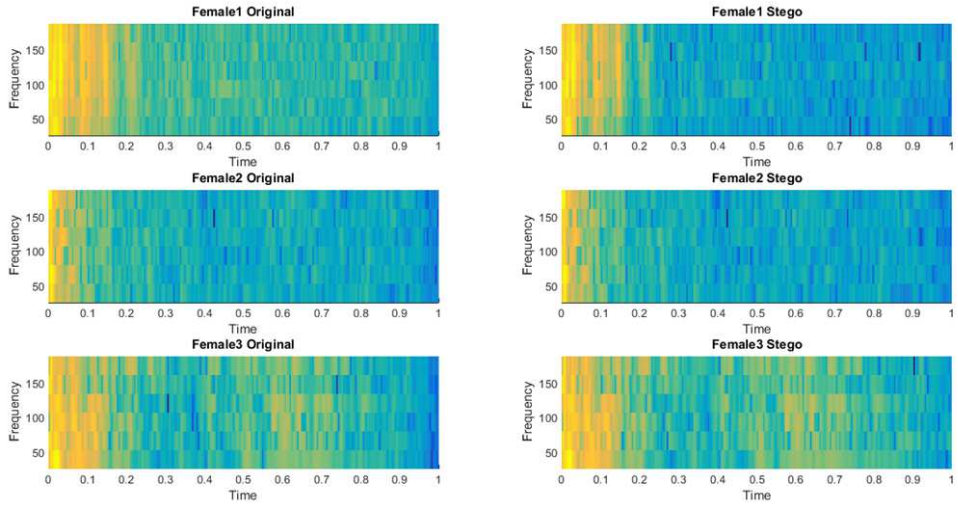

FIGURE 12. Spectrogram analysis of three female voices

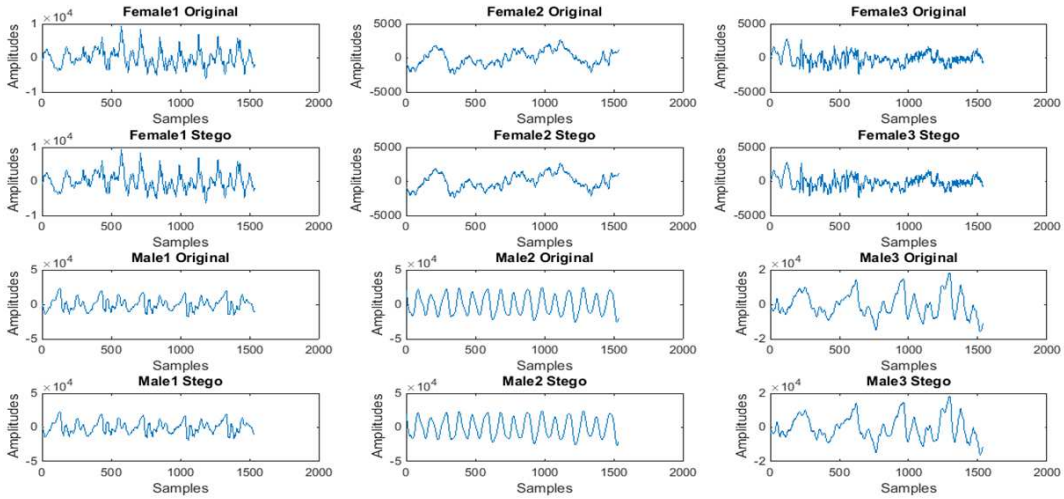

FIGURE 13. Time Domain analysis of original and stego signal

[6] Atta-ur-Rahman, K. Sultan, N. Aldhafferi, A. Alqahtani, M. Mahmud, Reversible and fragile watermarking for medical images, *Computational and Mathematical Methods in Medicine*, June 2018.

[7] Atta-ur-Rahman, K. Sultan, N. Aldhafferi, A. Alqahtani, D. Abdullah, M. Mahmud, Robust and fragile watermarking for medical images: A joint venture of coding and chaos theories, *Journal of Healthcare Engineering*, June 2018.

[8] Atta-ur-Rahman, M. Mahmud, K. Sultan, N. Aldhafferi, A. Alqahtani, D. Abdullah, Medical image watermarking for fragility and robustness: A chaos, ECC and RRNS based approach, *Journal of Medical Imaging and Health Informatics*, vol. 8, no. 6, pp. 1192-1200, July 2018.

[9] M. Zaheer, I. M. Qureshi, Atta-ur-Rahman, J. Alhiyafi, M. Z. Muzaffar, Improved and secure differential LSB embedding steganography, *Journal of Information Assurance and Security*, vol. 11, pp. 170-178, 2018.

[10] Atta-ur-Rahman, M. T. Naseem , M.Z. Muzaffar, Reversible and robust watermarking using residue number system and product codes, *Journal of Information Assurance and Security (JIAS)*, vol. 7, pp. 156-163, 2012.

[11] X. Huang, Y. Abe, & I. Echizen, Capacity adaptive synchronized acoustic steganography scheme, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 2, pp. 72-90, 2010.

[12] W. Bender, D. Gruhl, N. Morimoto, & A. Lu, Techniques for data hiding, *IBM systems journal*, vol. 35, (3.4), pp. 313-336, 1996.

[13] E. Ercelebi, & L. Batakci, Audio watermarking scheme based on embedding strategy in low frequency components with a binary image, *Digital Signal Processing*, vol. 19, no. 2, pp. 265-277, 2009.

[14] H. Wang, & S. Wang, Cyber warfare: steganography vs. steganalysis, *Communications of the ACM*, vol. 47, no. 10, pp. 76-82, 2004.

[15] J. Wang, R. Healy, & J. Timoney, A robust audio watermarking scheme based on reduced singular value decomposition and distortion removal, *Signal Processing*, vol. 91, no. 8, pp. 1693-1708, 2011.

[16] N. Cvejic, & T. Seppanen, Reduced distortion bit-modification for LSB audio steganography, *In Signal Processing, 2004. Proceedings. ICSP'04. 2004 7th International Conference on IEEE*, vol. 3, pp. 2318-2321, 2004.

[17] A. Delforouze, & M. Pooyan, Adaptive digital audio steganography based on integer wavelet transform, *Circuits, Systems & Signal Processing*, vol. 27, no. 2, pp. 247-259, 2008.

[18] S. S. Shahreza, & M. T. M .Shalmani, Adaptive wavelet domain audio steganography with high capacity and low error rate, *In Proceedings of the IEEE International Conference on Information and Emerging Technologies, (ICIET'07)*, pp. 1729-1732, 2007.

[19] S. S. Shahreza, & M. T. M. Shalmani, High capacity error free wavelet domain speech steganography, *In 2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1729-1732, 2008.

[20] H. I. Shahadi, & R. Jidin, High capacity and inaudibility audio steganography scheme, *In Information Assurance and Security (IAS), 2011 7th International Conference on IEEE*, pp. 104-109, 2011.

[21] H. I. Shahadi, R. Jidin, & W. H. Way, A novel and high capacity audio steganography algorithm based on adaptive data embedding positions, *Research Journal of Applied Sciences, Engineering and Technology*, vol. 7, no. 11, pp. 2311-2323, 2014.

[22] J.-S. Pan, W. Li, C.-S. Yang and L. J. Yan, Image steganography based on subsampling and compressive sensing, *Multimedia Tools and Applications*, vol. 74, no. 21, pp. 9191-9205, 2015.

[23] J.-S. Pan, J.-J. Duan, W. Li, A Dual Watermarking Scheme by Using Compressive Sensing and Subsampling, *ECC* pp. 381-389, 2015.