

New audio encryption package for TV cloud computing

Salwa M. Serag Eldin · Salah A. Khamis ·
Abdel-Aziz Ibrahim Mahmoud Hassanin ·
Mohammed A. Alsharqawy

Received: 5 September 2013 / Accepted: 15 September 2014 / Published online: 10 October 2014
© Springer Science+Business Media New York 2014

Abstract For any cloud computing (CIComp), encryption of multimedia is one of the main applications as cloud tries to maintain it in a good situation and protect from any tampering. This work provides a new technique for audio for TV cloud computing. Encrypting the audio signals is addressed based on chaotic map and the algorithm was tested using an audio tone (AT) to evaluate the performance. The software of encrypt audio using AT based on chaotic map is specially designed to meet the needs of CIComp of Egyptian Radio and Television Union (ERTU). The proposed software of CIComp of ERTU is practical in nature and aims to provide individuals with an understanding of how to create cutting-edge web applications to be deployed distributive across the latest hosting platforms of CIComp of ERTU, including public/hybrid CIComp of ERTU, peer-to-peer networks, clusters, and multi-servers.

Keywords Cloud computing · AuthGs · ERTU · DCT · DWT · DST · Chaotic map

S. M. S. Eldin · S. A. Khamis
Electronics and Electrical Communication Engineering
Department, Tanta University, Tanta, Egypt
e-mail: sserag@gmail.com

S. A. Khamis
e-mail: s.khamis@f-eng.tanta.edu.eg

A.-A. I. M. Hassanin
Electronics and Electrical Communication Engineering
Department, Faculty of Electronic Engineering,
Menoufia University, Menoufia, Egypt
e-mail: abdel_aziz_hassanin@hotmail.com

M. A. Alsharqawy (✉)
Egyptian Radio and Television Union (ERTU), Cairo, Egypt
e-mail: mnm_1946@hotmail.com

1 Introduction

Many methods are invented to present a good tool for encrypting audio signals. The attacker tries to know the secret key that used for encryption. One of the major characteristic for audio is presence of silent period in the signal, where the attacker try to find through it the keys as it is considered as cipher text its plaintext is known. The attacker can know the key. All methods try to hide this period that called residual intelligibility to give the process a robustness and high security. Also connecting this service with the cloud of ERTU via several methods like Wi-Fi and mobile is an important issue to address. One of this tool cipher an image and embed it in the right part of tracks and apply a transformation where is placed in left side of track. All this operation is biased on chaotic map [Yin and Min \(2010\)](#). Another algorithm is scramble audio file in multidimensional that give more security against attacks [Li et al. \(2009\)](#). Lessons learned on the usage of call logs for security and management in Internet Protocol (IP) Telephony is described in [Tartarelli et al. \(2010\)](#). Balance of security strength and energy for a phasor measurement unit (PMU) monitoring system in smart grid is presented in [Qiu et al. \(2012\)](#). Toward secure targeted broadcast in smart grid is offered [Fadlullah et al. \(2012\)](#). Network access security for the internet: Protocol for carrying authentication for network access is provided [Marin-Lopez et al. \(2012\)](#). The Euler project: Application of software defined radio in joint security operations is demonstrated [Baldini et al. \(2012\)](#). Security and network operations challenges with cellular infrastructure in the tactical theater are attributive [Elmasry et al. \(2012\)](#). Physical layer security in wireless smart grid is depicted [Lee et al. \(2012\)](#). Secure service provision in smart grid communications is decrypted [He et al. \(2012\)](#). Secure wireless communication system for smart grid with rechargeable electric vehicles is capacitated [Su et al. \(2012\)](#). Synchronized multi-

media streaming on the iPhone platform with network coding is made [Vingelmann et al. \(2011\)](#). A new tutorials on IEEE 802.1AS is provided that updates earlier description, and new simulation results for timing performance for synchronization of audio/video bridging networks [Garner and Ryu \(2011\)](#). A survey is done some of the prevalent and upcoming backhaul technology trends based on the aforementioned evolution within RAN. Wherever possible, a critical analysis of particular technology trend for its technical and commercial feasibility is also presented [Raza \(2011\)](#). The cloud computing of the television has been used to broadcast live TV to cell phones via satellite, terrestrial towers or Wi-Fi networks. Land-based broadcasting techniques send out analog or digital TV signals over the air from terrestrial base stations. The mobile telephone with a TV antenna and an analog or digital TV tuner can pick up the signals ([Yasumoto et al. 2011](#); [Polák and Kratochvíl 2011, 2012](#); [Eldin et al. 2013](#); [Tamayo-Fernández et al. 2011](#); [Constantiou and Mahnke 2010](#)). Some standards rely on satellite broadcasting to deliver live TV to cell phones. They can broadcast from satellite to mobile telephone, from satellite to base station to phone or use both techniques simultaneously [Iqbal and Ahmed \(2011\)](#). This broadcast method streams live TV signals via the Internet. A web-enabled smartphone with data capabilities can pick up the stream from any Wi-Fi hotspot or WiMAX coverage area ([Högberg 2010](#); [Mierau et al. 2011](#)). The rest of this paper is organized as follow. Section 2 presents the software package proposed for ERTU cloud computing. Software package with Chaotic and Multiple Key (MK) encryption results are given in Sects. 3 and 4 respectively, taking noise effect

into consideration. Finally section V is the conclusion of the paper.

2 The proposed software package for audio encryption of CICOMP

Figure 1 shows the layout of audio encryption proposed for ERTU cloud. This layout indicates the flow of the audio through the proposed package during processing. The graphical user interface for the proposed package is shown in Fig. 2. As shown, the package contains five pools as follows:

Scenario user can choose the multimedia to be protected or transmitted.

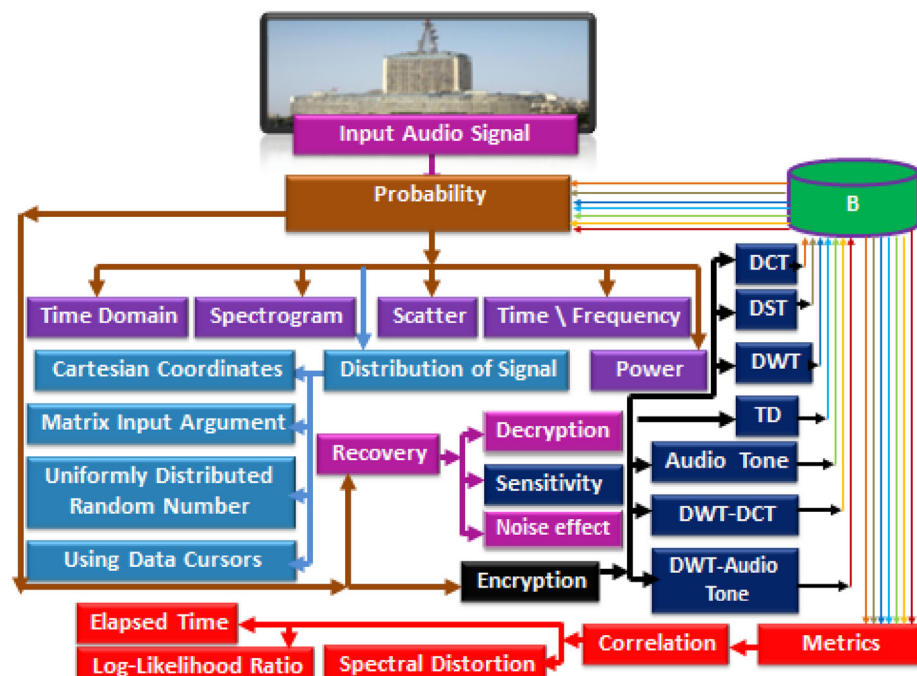
Flowcharts in which user can monitor the main characteristics of the audio such as time domain, spectrogram, power, time/frequency and signal distribution.

Encryption in which the audio is to be encrypted by either chaotic or MK algorithm. The package supports many transforms such as discrete cosine transform (DCT), discrete wavelet transform (DWT) and discrete sine transform (DST). The package also presents a new technique using AT, to be discussed later.

Recovery The audio is recovered by AuthGs through the recovery process.

Metrics many metrics are supported by the package such as elapsed time, log-likelihood ratio (LLR), correlation, and spectral distortion (SD) to enable user to guarantee protection and security.

Fig. 1 The layout of audio encryption that used in ERTU cloud



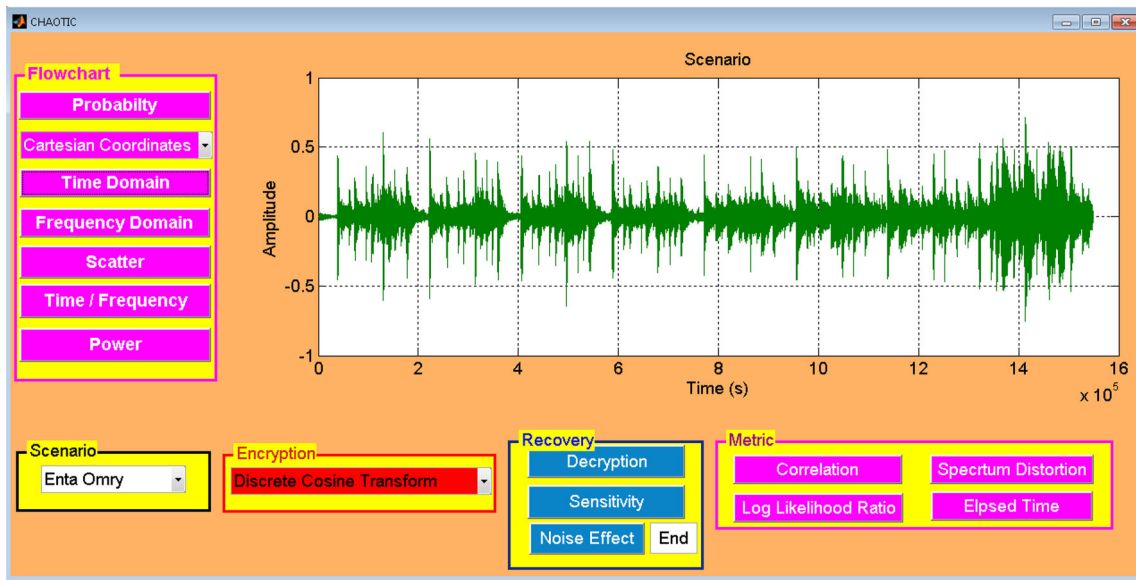


Fig. 2 Software package GUI of audio encryption proposed for ERTU cloud

Spectrogram is a graph which indicates the frequencies of speech versus time. It is used to get visual indication and comparison between the original and processed audio. Distribution of the signal gives the distribution of the signal’s amplitude and it becomes a good comparison tool between processed and original speech. Histograms show the distribution of data values across a data range. It may be divided to many categories

Scatter plots (also called scatter diagrams) are used to investigate the possible relationship between two variables that both relate to the same “event.” A straight line of best fit (using the least squares method) is often included. The scatter diagram helps to identify the existence of a measurable relationship between two items by measuring them in pairs and plotting them on a graph.

SD in the frequency variant spectral distance measure the likelihood pole coefficient (LPC) smooth spectrum of speech in the 300–3400 Hz band is divided into six bands and individual spectral distances are then computed over each band .In another way, it measure the distance between the original signal and the processed in frequency domain. It simply evaluates squared difference of the log-magnitude functions over an appropriate frequency band (Sridharan et al. 1991; Hedelin et al. 1999). It can be calculated as:

$$SD_{v_0}^2 = \frac{1}{2v_0} \int_{-v_0}^{v_0} \left(10 \log_{10} \left| A \left(e^{j2\pi v} \right) \right|^2 - 10 \log_{10} A e^{j2\pi v} \right)^2 dv \tag{1}$$

where $1/A(z)$ is a filter model and $1/\hat{A}(z)$ is its quantized correspondent

LLR is a measure of spectral similarity between two signals and it has found wide use in areas of speech recogni-

tion and verification (Crochiere et al. 1950; Tribolet et al. 1978). The principal assumption on which the LLR distance is based on that speech can be represented by a p th order all-pole model of the form:

$$x(n) = \sum_{m=1}^p a_m x(n-m) + G_x u(n) \tag{2}$$

where $x(n)$ is the sampled speech signal, $a_m (m = 1, 2, \dots, p)$ are the coefficients of an all-pole filter $1/A_x(z)$, which models the resonances of the speech production mechanism G , is the gain of the filter, and $u(n)$ is an appropriate excitation source for the filter. The waveform coder can be represented in which $x(n)$ is the input speech, which can be modeled according to (2), and $y(n)$ is the decoded output. The LLR log for comparing $x(n)$ and $y(n)$ can then be defined as:

$$l = \log \left[\frac{a_x R_y a_x^t}{a_y R_y a_y^t} \right] \tag{3}$$

where

a_x = LPC coefficient vector $(1, a_1, a_2 \dots a_p)$ for the original speech $x(n)$,

a_y = LPC coefficient vector $(1, G_1, G_2 \dots G_p)$ for the coded speech $y(n)$

And R , is the correlation matrix of $y(n)$

Correlation is known as how much the similarity as identically between the original speech and the processed, and is given by Naem et al. (2009):

$$C = \frac{\sum_{r=1}^H \sum_{c=1}^W (I_1(r, c) - \bar{I}_1) (I_2(r, c) - \bar{I}_2)}{\sqrt{\left[\sum_{r=1}^H \sum_{c=1}^W (I_1(r, c) - \bar{I}_1)^2 \right] \left[\sum_{r=1}^H \sum_{c=1}^W (I_2(r, c) - \bar{I}_2)^2 \right]}} \tag{4}$$

where $I_1(r, c)$ is the value of the pixel at the point (r, c) in the original audio. $I_2(r, c)$ is the value of pixel at (r, c) in the encrypted audio, \bar{I}_1 is the mean of the original audio and \bar{I}_2 is the mean of the encrypted audio that is calculated as follows

$$\bar{I} = \frac{1}{W * H} \sum_{r=1}^H \sum_{c=1}^W I(r, c) \quad (5)$$

Sensitivity The degree of affecting is called the sensitivity, if the process is affected by a small change, so its sensitivity is high and vice versus.

A new algorithm for audio encryption is also proposed and applied via the package. The new algorithm based on encrypting the audio signal, then an AT is used with a mathematical operation to test and assure the encrypted signal is free from residual intelligibility hence increase the security. Audio encryption is done through both Chaotic and (MK) algorithms.

2.1 Encryption process

The package supports two types of encryption techniques, chaotic and MK algorithms. In chaotic algorithm, the audio signal is permuted by chaotic algorithm using an initial key then applies any transform to the resulted signal to apply a second permutation where the three level of permutation will be done on the processed signal. A masking step is done to assure that the value of each element not over 2 where it insures there is no silent period as possible.

Chaotic map is an encryption algorithm that used to relocate the position data into position. It has the benefit of low correlation, good randomness and non-predictability. It has, also a high sensitivity to initial parameters, that if as small change has been occurred [Naeem et al. \(2009\)](#).

The general equation is:

$$B(x, y) = \begin{cases} (2x, y/2) & 0 \leq x < \frac{1}{2} \\ (2x - 1, \frac{y}{2} + \frac{1}{2}) & \frac{1}{2} \leq x \leq 1 \end{cases} \quad (6)$$

But we use key for initial condition so as to perform the encryption algorithm. Generalized Baker map can be generalized as follows:

- An $N \times N$ square matrix is divided into k vertical rectangles of height N and with width n_i , where $n_1 + n_2 + \dots + n_k = N$.
- These vertical rectangles should be stretched horizontally.
- Then, the rectangles are stacked to have the left one at the bottom and the right one at the top.

Discretized Baker map will be denoted $B(n_1, n_2, \dots, n_k)$, where the sequence of k integers, n_1, n_2, \dots, n_k , is chosen, such that each integer n_i divides N , and $N = n_1 + \dots + n_i$.

The digit at the position (r, s) , with $N_i < r < N_i + n_i$ and $0 < s < N$ is mapped to

$$B_{(n_1 \dots n_k)}(r, s) = \left[\frac{N}{r}(r - N_i) + s \bmod \left(\frac{N}{n_i} \right), \frac{n_i}{N} \left(s - s \bmod \left(\frac{N}{n_i} \right) \right) + N_i \right] \quad (7)$$

An $N \times N$ square matrix is divided into k vertical rectangles of height N and with width n_i . Then, each vertical rectangle of dimensions $N \times n_i$ is divided into n_i boxes; each containing N points. Each of these boxes is mapped to a row of pixels by mapping column by column, with the left one at the bottom and the right one at the top.

In MK algorithm, several keys are based on one key then generate the other key from it. In this work, a second key is the inverse of original key by divided it to two halves and reverse each to generate new key. Another key is used to make block and randomization of the data, by using this key to permuted the signal. Any transformation is used to apply second permutation followed by inverse transformation. First, block randomization changes the position of any elements in the matrix to another position using the keys generated before. The matrix is divided into blocks equal to the length of keys then applies a row and column randomization where if the value of key element equal zero then the row or the column has no change. If the value of key is equal to one, then the shift for row or column is equal to the number of previous one in the key. After that, a masking step is done to assure that the value of each element not over 2.

2.2 Package applications

2.2.1 Visual inspection

The proposed package enable user to visually inspect the media under processing. For package testing, the Osarry's voice is used for six seconds long. Figure 3(a–f) shows time domain signals for original, encrypted, recovered and frequency domain signals for original, encrypted and recovered respectively. The figure shows the difference between the original signal and the encrypted one, besides the clear of Residual intelligibility also similarity between original and recovered signal can be verified.

Package also supports signal distribution that are shown in Fig. 4, where it indicates the difference in the distribution of the amplitude between the original and encrypted signal besides showing the close similarity between the original and recovered signal.

The scatter diagram, shown in Fig. 5 indicates the correlation between the original signal and both the encrypted and decrypted signal, the figure indicate the high correlation for decryption and low in case of encryption. It also indicates the scattering region between the original sig-

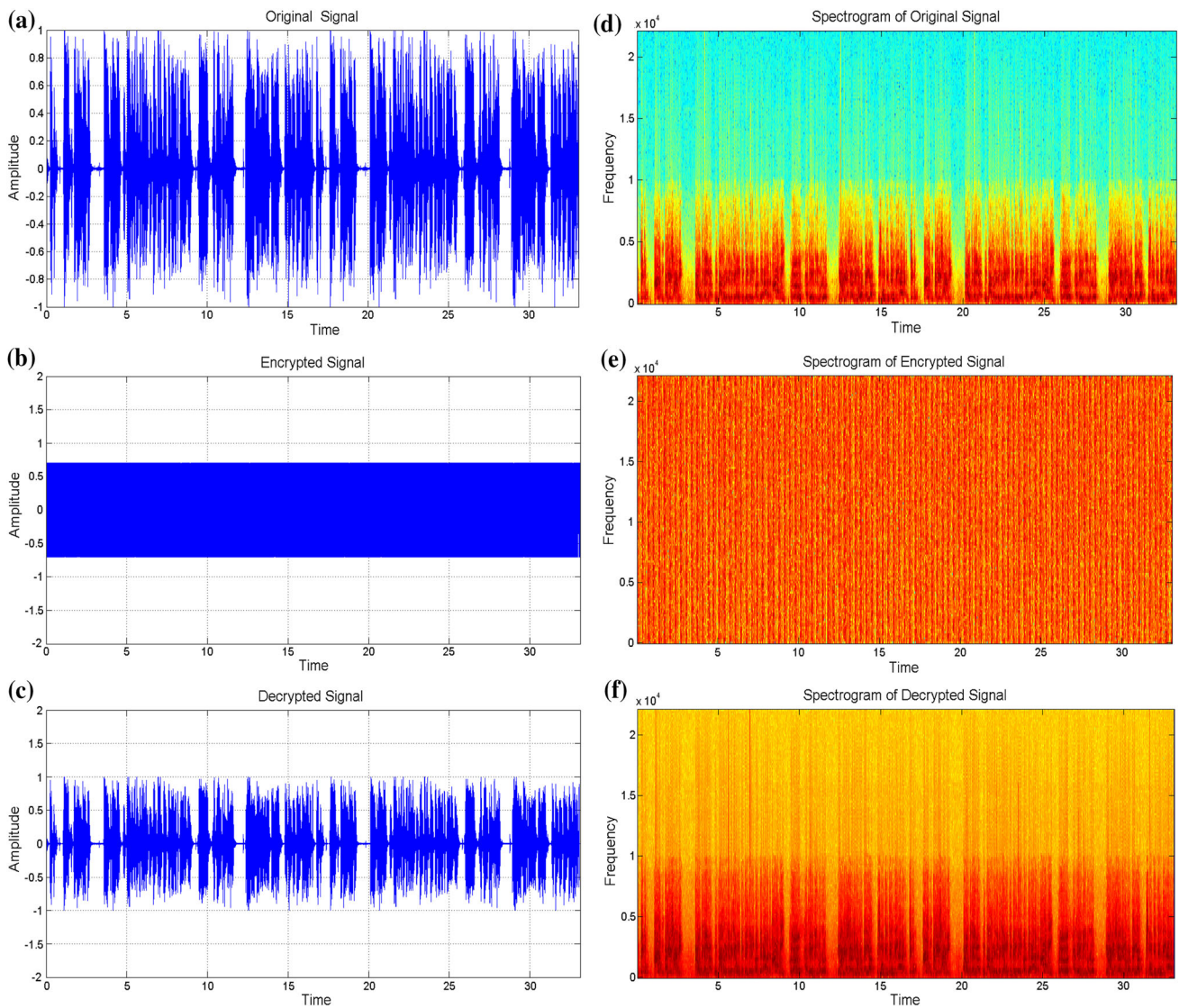


Fig. 3 Time domain signals **a** original, **b** encrypted and **c** recovered and Frequency domain signals **d** original, **e** encrypted and **f** recovered

nal and the recovered as well as the encrypted one where it is a sign for a relation between both signal and how it is difficult to get it from. The correlation between the original and encrypted signal is -7121×10^{-004} and the between the original and the recovered signal equal 1. The SD in encryption is 17.0025 dB where in the decryption is 2.2546×10^{-010} dB. LLR of the encryption is 0.8124 and in the decryption is 2.7513×10^{-014} . The LLR describes the same results where is big in case of the original and encrypted and very small in case of original and decrypted signals.

2.2.2 Key sensitivity test

The package also was tested against key change to guarantee cloud security. One bit change in the key was deliber-

ately changed. Figure 6 shows the difference between the original and the decrypted signal where a small change in the decrypted key occurred. It gives good evidence to how the system is sensitive to any change in the keys and hence guarantees security. Studying the quality metrics in this case shows that the correlation between the original and decrypted signal is 0.1276 and describes the dissimilarities between them. The same results can be considered in the value of SD and LLR where it is 126.1073 dB and none respectively.

2.2.3 Noise effect

The effect of noise was also evaluated for many metrics. Output SNR, segmental SNR, correlation, LLR and SD are calculated in different case of input SNR. The 100 dB for input

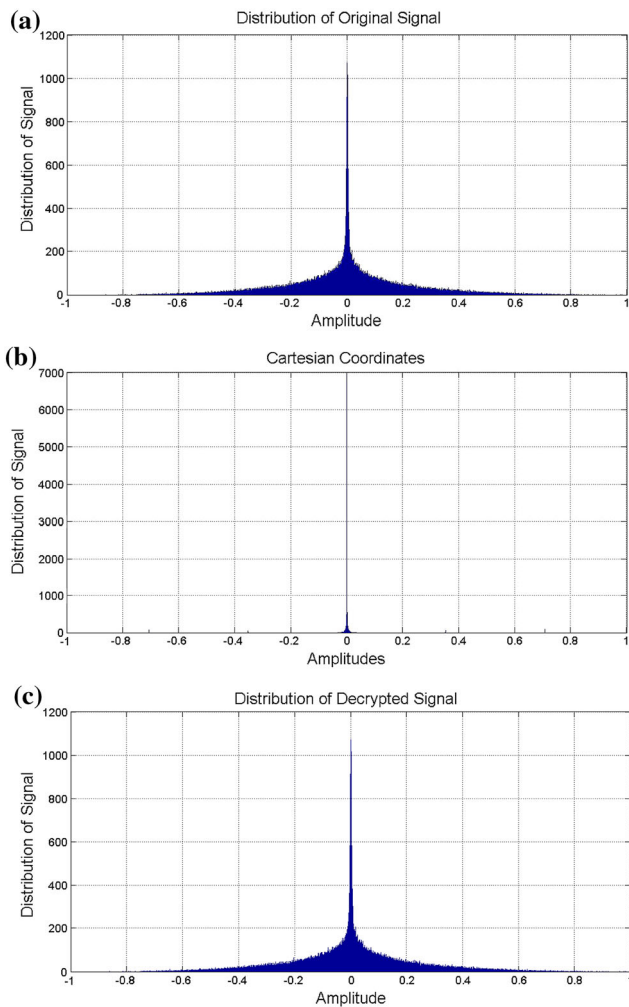


Fig. 4 The distribution of signal **a** original **b** encrypted **c** decrypted

SNR is used to evaluate the different metrics. In Fig. 7.e, the correlation indicates that the increase in SNR value increase the correlation and it increase linearly. Segmental SNR shows an increase in its value with increase SNR value in almost linear manner as shown in Fig. 7a. For Fig. 7b, Output SNR has the same behavior as previous metrics. LLR shows a variation with decrease in its value. In case of SD test the value decrease as based on Fig. 7c, d. So, this technique gives a good condition of encryption for medium and high SNR, and become good case at 15 dB. The variation in LLR is in small range, Segmental SNR and Output SNR vary in range of 20 dB. Correlation and SD’s variation is very big range.

2.2.4 Audio tone

In this work, a new algorithm is proposed to encrypt the audio signal by using Chaotic encryption, then use an AT by an mathematical operation to test and assure the encrypted

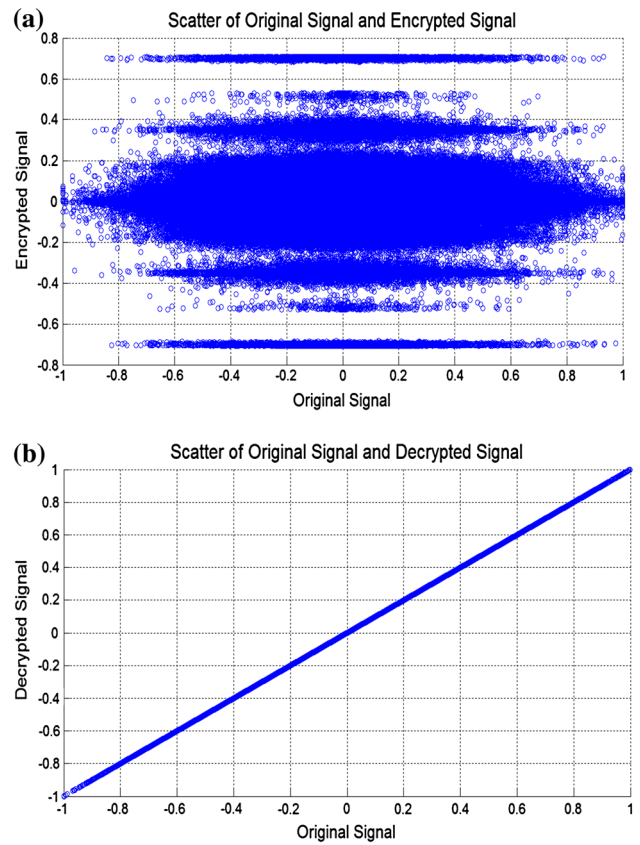


Fig. 5 The scattering between the original signal and **a** encrypted, **b** decrypted

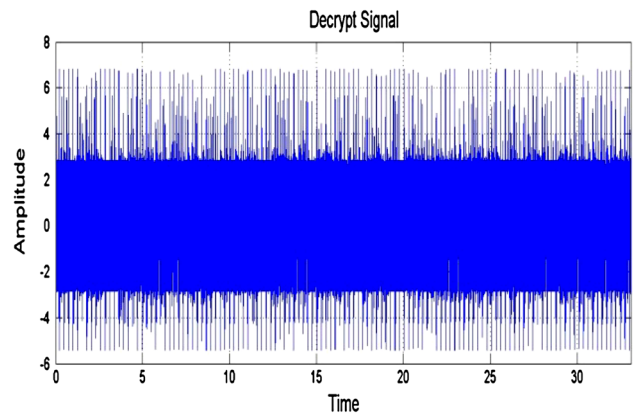


Fig. 6 The time domain of the decrypted signal for case of change in keys

signal is free from residual intelligibility, so increase the security of the signal from hacking eavesdrops groups and non AuthGs. The resulted signal from second chaotic encryption stage is compared by certain level and makes a decision. If the level is small than threshold, a arithmetic operation is done where it is added to the tone signals. Otherwise, the reverse of these operations is performed for the signals which it is subtracted from tone signal.

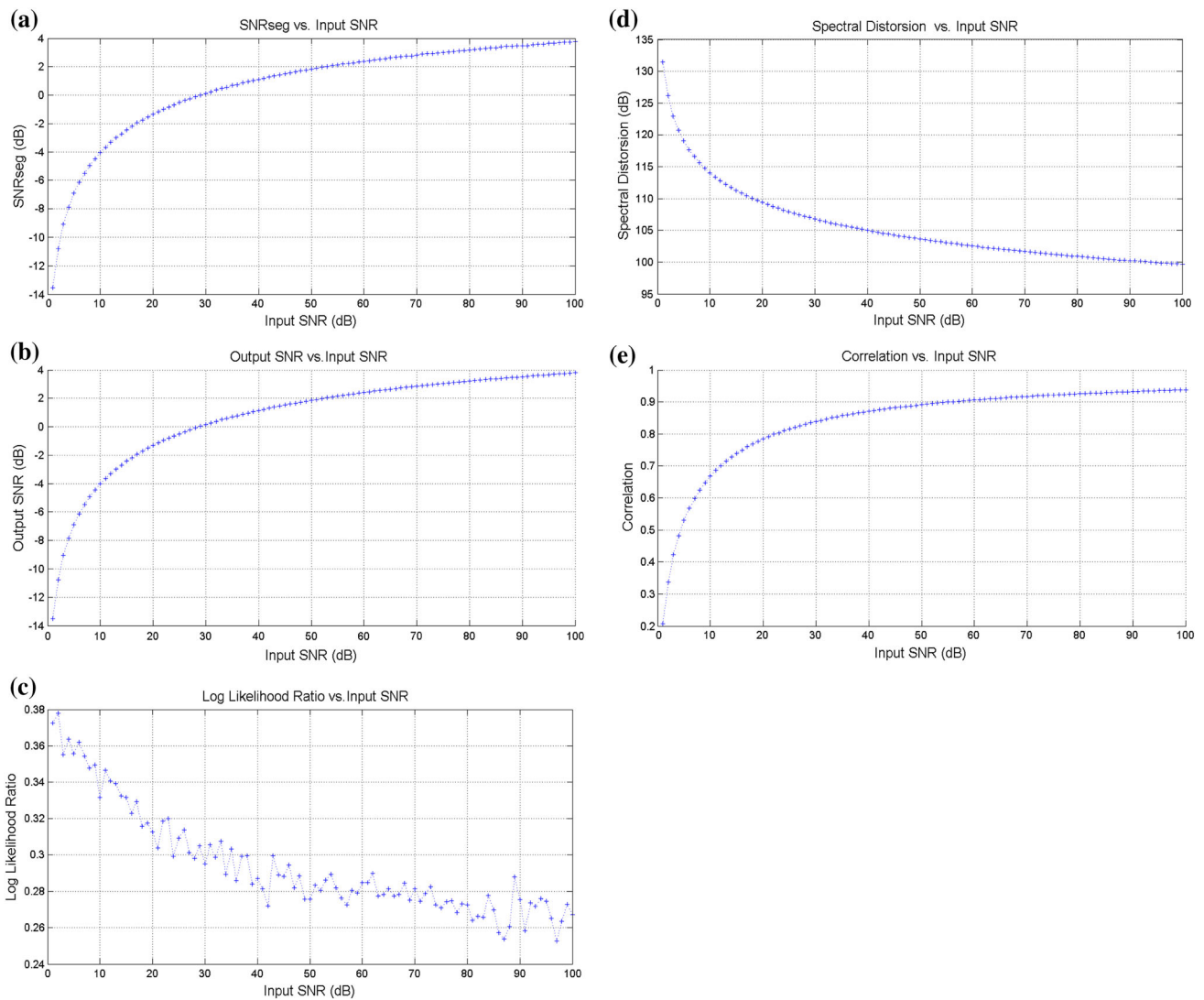


Fig. 7 Effect of the noise in the decrypted signal **a** segmental SNR, **b** output SNR, **c** log-likelihood ratio, **d** spectral distortion and **e** correlation

For AT proposed testing, the Osarry’s voice is used to test the algorithm for six seconds long and the Osarry’s voice is used as tone. Figure 8a and b show time domain voice and AT signals respectively. Encrypted signal with AT algorithm and recovered one is shown in Fig. 8c and d respectively. From Fig. 8, it is obvious that the difference between the original signal and the encrypted one, besides showing the clear of Residual intelligibility and the similarity between the original and recovered signal can be verified.

The scattered diagram between the original signal and both the encrypted and decrypted signal is shown in Fig. 9 that indicates the high correlation for decryption and low in case of encryption.

AT algorithm was also tested against key sensitivity. Figure 10 shows the difference between the original and the decrypted signal where a small change in the decrypted key

occurred. It gives a good example to how the system is sensitive to any change in the keys.

Table 1 gives more information for the different criteria for all supported transforms. Different metrics are available to help user to choose the desired transform.

3 Multiple keys results

Another similar software package for audio encryption with MK algorithm is also presented. All visual inspection tests and metrics described before are also available in that package. Here in a comparison between chaotic and MK encryption algorithms is presented. The performance of each algorithm is investigated in case of noise existence as well as processing time. DWT and proposed AT are also compared. Segmental SNR, Output SNR, LLR, SD and Correlation were

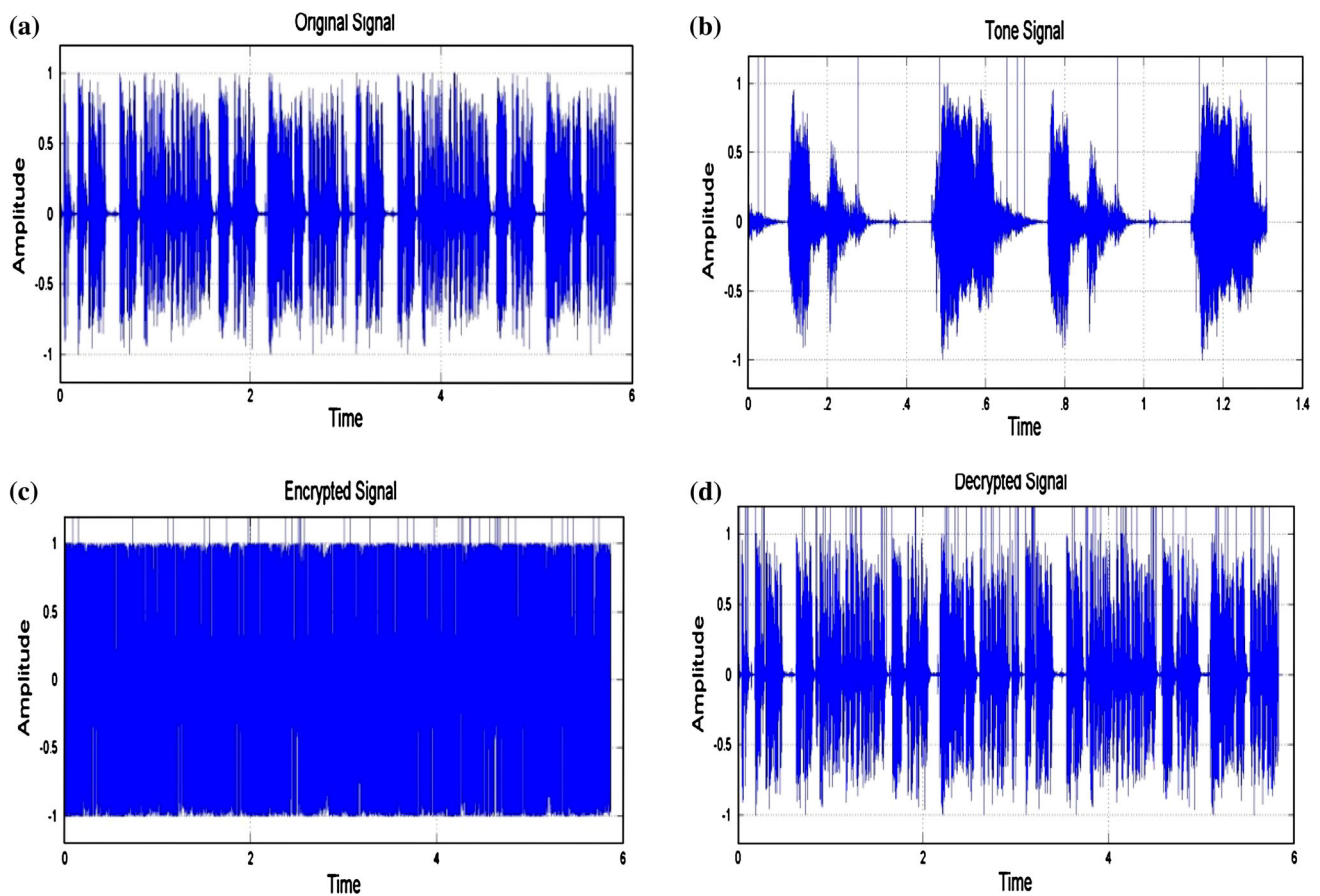


Fig. 8 Osarry's Time domain as **a** original signal, **b** AT used in encryption, **c** encrypted signal and **d** recovered signal

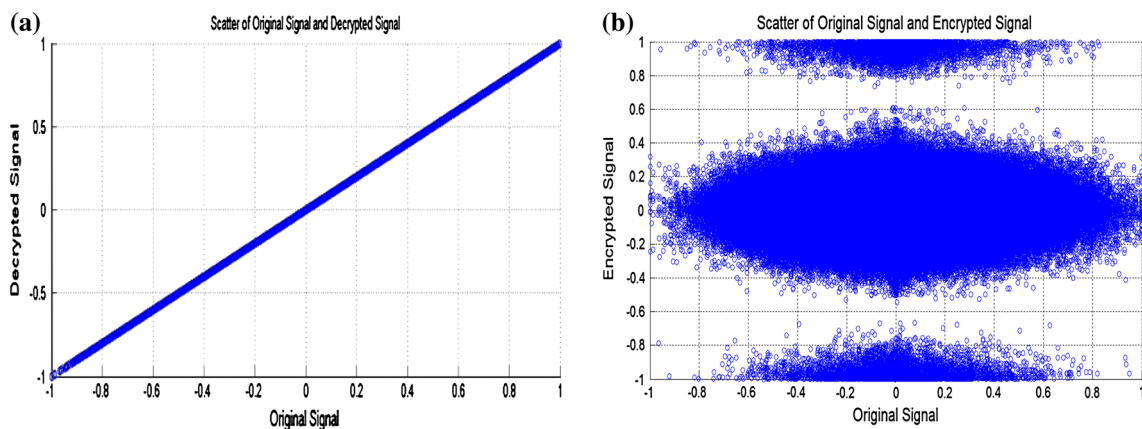


Fig. 9 Scattering between the original signal and **a** decrypted, **b** encrypted

of the decrypted signal were investigated. Figure 11. a shows that for segmental signal to noise ratio, chaotic encryption gives higher segmental signal to noise ratio than MK algorithm.

In the following, the effect of noise will be evaluated for many metrics. Output SNR, segmental SNR, correlation, LLR and SD are calculated in different case of input SNR.

The 100 dB for input SNR is used to evaluate the different metrics. The test is done for both chaotic map and MKs for DWT and AT. The segmental SNR is a metric used to evaluate the effect of noise for the encrypted signal and how to effect for the decrypted signal. It evaluates the SNR for certain frame of the signal. In Fig. 11a, DWT in chaotic increase smoothly until to be fixed in its output value at 60 dB where

Fig. 10 Time domain of the decrypted signal in case of key change

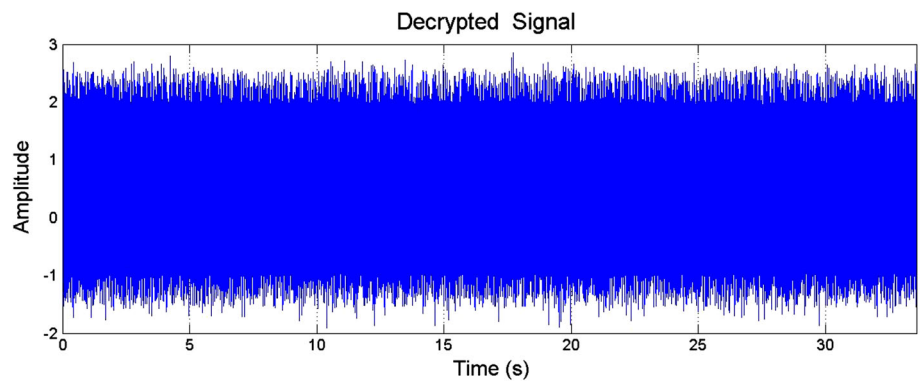


Table 1 The different metrics for all supported transforms

Transform	Encryption			Decryption			Sensitivity Test		
	Correlation	SD	LLR	Correlation	SD	LLR	Correlation	SD	LLR
DCT	-0.0039	17.1058	0.5098	0.9982	0.4120	0.0429	0.1950	15.1107	0.6637
DST	-0.0018	15.2681	0.4736	0.9420	5.6866	0.4959	0.0588	14.9361	0.4170
DWT	1.1103×10^{-5}	24.7824	0.6549	1	1.1701×10^{-14}	4.8932×10^{-13}	0.2013	22.4181	NaN
AT	0.0069	17.0587	1.1486×10^3	1	2.5831×10^{-15}	1.3508×10^{-09}	0.1959	14.5307	0.7371

AT in chaotic has a peaks in first value of SNR and become decrease which start to be fix after 60 dB but with small variation in its value. AT in MK is almost constant with change of SNR but its result is very bad and DWT in MK is decrease sharply and become constant after 2 dB. It is also has bad response. In Segmental SNR, AT in chaotic is preferred in low SNR where DWT in chaotic is powerful than AT due to its stability in the value. The MK performs badly for all value of SNR. The output SNR calculates the SNR for the whole signals with SNR change which is showed in Fig. 11b. DWT in chaotic increase smoothly until to be fixed in its output value at 60 dB where AT in chaotic increase linearly and start to be constant after 40 dB but with noticeable variation in its value. AT in MK is almost constant with change of SNR but its result is very bad and DWT in MK is decrease sharply and become constant after 2 dB. It is also has bad response. In Output SNR, AT in chaotic is preferred but being careful for high SNR where DWT in chaotic is less than AT but has the advantage of its stability in the value. The MK performs badly for all value of SNR. In Fig. 11c, the SD gives the effect of SNR for the similarity of decrypted signal with the original. Increase the value of SD is preferred in encryption and the reverse in decryption case. DWT in chaotic decreases linearly where AT in chaotic decrease smoothly and start to be constant after 50 dB. AT in MK is almost constant with change of SNR but its result is very bad and DWT in MK increase sharply and become constant after 2 dB. It is also has bad response. In SD, AT in chaotic is preferred where DWT in chaotic is the worst in high SNR than others. LLR is another metric to describe how much the processed signal

close to the original. Increase the value of LLR is preferred in encryption and the reverse in decryption case. DWT in chaotic decreases in small range with variation where AT in chaotic decrease and start to be constant after 55 dB. AT in MK increase with variation until become constant at 50 dB and DWT in MK increase sharply and become constant after 2 dB. In LLR, AT in chaotic is the worst where AT in MK is preferred in high SNR than others and DWT in MK preferred in low SNR. All of them are represented in Fig. 11d. The correlation and its effects with SNR is displayed in Fig. 11e. DWT in chaotic increase almost linearly and start to be fixed after 60 dB where AT in chaotic increase almost linearly and start to be constant after 20 dB. AT in MK is constant with change of SNR value and DWT in MK decreases sharply and become constant after 2 dB. In correlation, AT in chaotic is the best where DWT in MK is the worst. MK has bad response of for all SNR value. AT in chaotic is the preferred than other and DWT in chaotic become the second choice.

Figure 12a monitors that the variation of block size’s effect on correlation shows that the similarities between all techniques except AT in case of Chaotic encryption which the correlation varies with change of block size. The LLR’s responses for all techniques almost have the same response with slight different in its value in case of AT Chaotic encryption as represented in Fig. 12b. For SD, Fig. 12c highlights that the MK encryption has the same response while the AT in Chaotic Map has the smallest value. DWT is the largest of them and gives the best response. The time elapsed in the process for all techniques is the same especially after block size of 32 as described in Fig. 12d

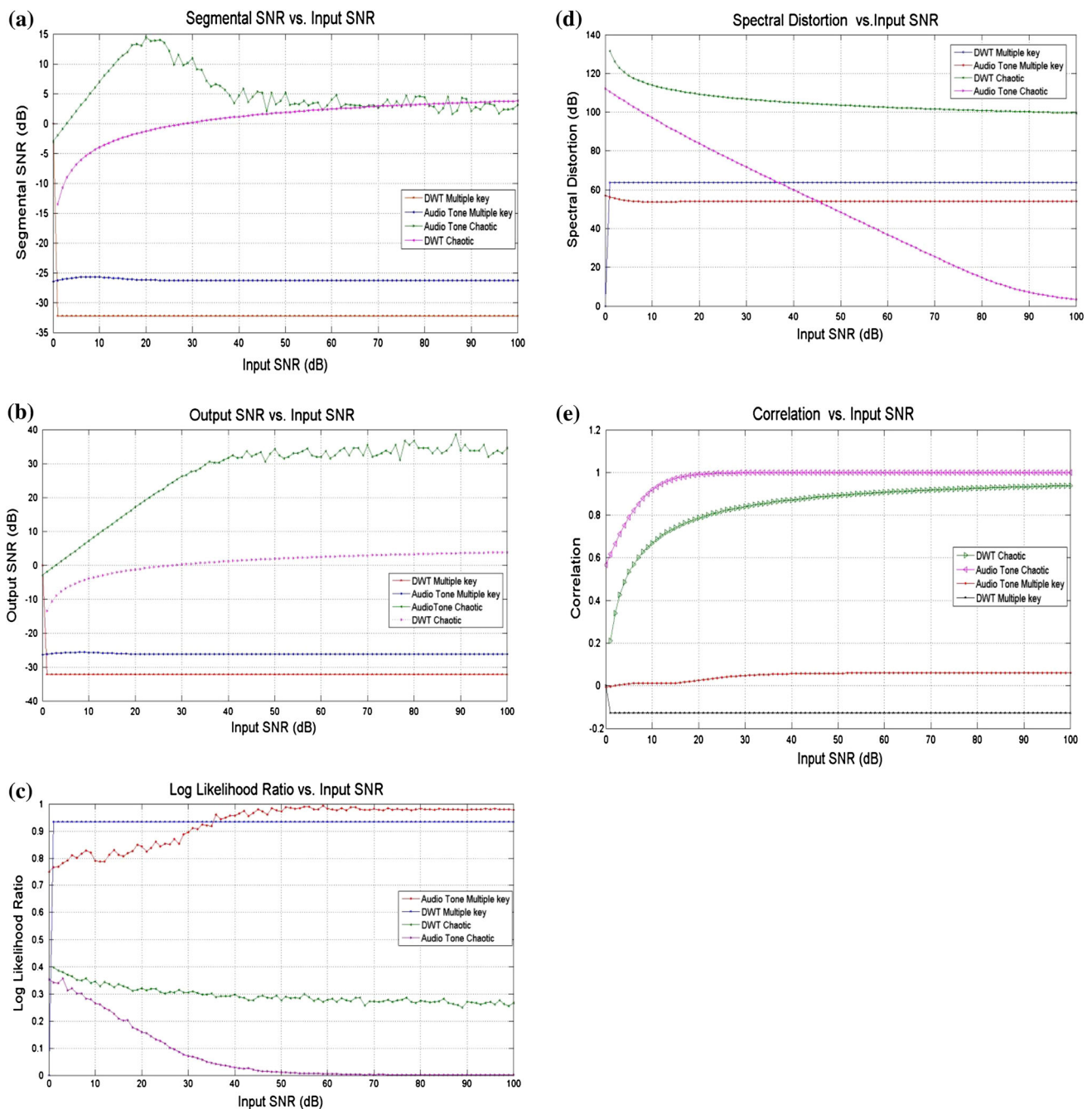


Fig. 11 Effect of the noise in the decrypted signal versus chaotic and MK algorithm **a** segmental SNR, **b** output SNR, **c** LLR, **d** SD and **e** correlation

4 Conclusion

Saving the audios and multimedia of encrypt Audio using AT Based on Chaotic Map is presented. One of important aspects that any media organizations try to maintain to protect its content from any attacks like stealing or modifying or reuse without permission in advance is provided. For any CComp, encryption of multimedia is one of application that cloud tries to maintain in good situa-

tion and protect from any tampering. In audio case, there are two type for protect the content according to its situation. First situation in the case broadcast the content and want not be received unless the AuthGs. Audio must be encrypted in way that if any one hears the encrypted signal can't recognize the content and so can't reuse or benefit from it. The second situation is to save it inside the organization's CComp with taking in consideration that may be abused by internal employee. Encrypting of the audio

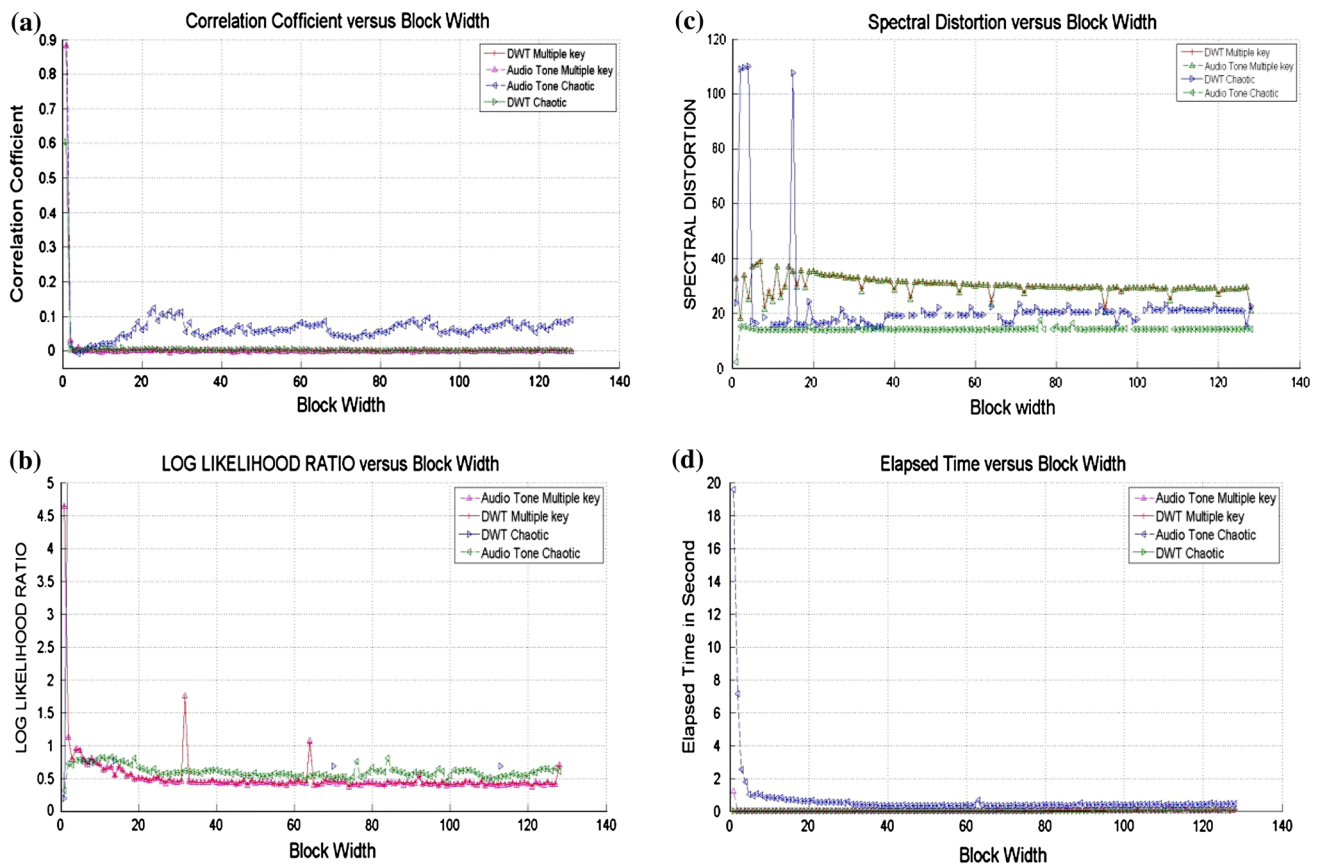


Fig. 12 The effect of block size with **a** correlation, **b** LLR, **c** SD and **d** elapsed time

signals is addressed based on chaotic map and test this algorithm by using an AT to evaluate the performance. As noticed from results, DWT and AT in Chaotic encryption have a good performance than other transforms. DWT has a good response and high security but AT has high robustness for noise than others. In MK encryptions, DWT perform well more than others, but all has a bad response with noise.

The software of encrypt audio using AT Biased on Chaotic Map should appeal to not only skilled CIComp of ERTU, but also those with an interest in applying web technologies to their organization. This software is therefore for experienced ICT professionals in the workplace and authorized will be able to:

- (a) Create and deploy a web application.
- (b) Use both enterprise and web application frameworks.
- (c) Build scalable web applications and analyses their performance using the latest tools and techniques.
- (d) Develop internet rich applications using the latest rich internet application frameworks.
- (e) Perform usability testing on a given web application to ensure maximum effectiveness.
- (f) Design and deploy wire framing, eye tracking and web analytics for web sites.

- (g) Generate a suitable business case to justify a web-based development.

References

- Baldini, G., Picchi, O., Luise, M., Sturman, T. A., vergari, F., Moy, C., et al. (2012). The euler project: Application of software defined radio in joint security operations. *IEEE Communications Magazine*, 50(3), 55–71.
- Constantiou, I. D., & Mahnke, V. (2010). Consumer behaviour and mobile TV services: Do men differ from women in their adoption intentions? *Journal of Electronic Commerce Research*, 11(2), 127–139.
- Crochiere, R. E., Tribolet, J. M., & Rabiner, L. R. (1950). An interpretation of the log likelihood ratio as a measure of waveform coder performance. *IEEE Transactions on Acoustics, Speech, and Signal Processing, ASSP-25*(3), 315–323.
- Eldin, S. M. S., Khamis, S. A., Hassanin, A.-A. I. M., Alsharqawy, M. A. (2013). ERTU's package for gray image watermark application. *Journal of Selected Areas in Telecommunications (JSAT)*, October Edition, 2013.
- Elmasry, G. F., Jain, M., Welsh, R., Jakubowski, K., & Wittaker, K. (2012). Security and network operations challenges with cellular infrastructure in the tactical Theater. *IEEE Communications Magazine*, 50(3), 72–80.
- Fadlullah, Z. Md., Kato, N., Lu, R., Shen, X. (Sherman), & Nozaki, Y. (2012). Toward secure targeted broadcast in smart grid. *IEEE Communications Magazine*, 50(5), 150–156.

- Garner, G. M., & Ryu, H. (Eric). (2011). Synchronization of audio/video bridging networks using IEEE 802.1AS. *Communications Magazine, IEEE, 49*(2), 140–147.
- He, D., Chen, C., Bu, J., Chan, S., Zhang, Y., & Guizani, M. (2012). Secure service provision in smart grid communications. *IEEE Communications Magazine, 50*(8), 52–61.
- Hedelin, P., Norden, F., & Skoglund, J. (1999). SD optimization of spectral coders. In *IEEE Workshop on Speech Coding Proceedings*, 28–30.
- Högberg, J. (2010). Mobile Provided Identity Authentication on the Web. http://projectliberty.org/liberty/content/download/4315/28869/file/WPBridgingIMS_AndInternetIdentity_V1.0.pdf. Accessed July 2013.
- Iqbal, A., & Ahmed, K. M. (2011). A hybrid satellite terrestrial cooperative network over non identically distributed fading channels. *Journal of Communications, 6*(7), 581–589.
- Lee, E.-K., Gerla, M., & Oh, S. Y. (2012). Physical layer security in wireless smart grid. *IEEE Communications Magazine, 50*(8), 46–52.
- Li, R., Qin, Z., Sha, L., Wang, B. (2009). A novel audio scrambling algorithm in variable dimension space, Feb. 2009, (pp.1647–1651).
- Marin-Lopez, R., Pereniguez, F., Gomez-Skarmeta, A. F., & Ohba, Y. (2012). Network access security for the internet: Protocol for carrying authentication for network access. *IEEE Communications Magazine, 50*(3), 84–92.
- Mierau, G., Aachen, R., Sträßer, M. & Aachen, R. (2011). Mobile Native vs. Web-based Learning Applications: A comparison between two modern mobile learning approaches, 8. <http://www.netmarketshare.com/browser-market-share.aspx?qprid=2&qpcustomd=1&qptimeframe=Y> (report generated November 25, 2011)
- Naeem, E. A., AbdElnaby, M. M., & Hadhoud, M. M. (2009). Chaotic image encryption in transform domains. *IEEE, 71*–76.
- Polák, L., & Kratochvíl, T. (2011). Analysis and simulation of the transmission distortions of the mobile digital television DVB-SH Part 1: Terrestrial mode DVB-SH-A with OFDM. *Radioengineering, 20*(4), 952–960.
- Polák, L., & Kratochvíl, T. (2012). Analysis and simulation of the transmission distortions of the mobile digital television DVB-SH Part 2: Satellite Mode DVB-SH-B with TDM. *Radioengineering, 21*(1), 126–133.
- Qiu, M., Su, H., Chan, M., Ming, Z., & Laurence, T. (2012). Balance of security strength and energy for a PMU monitoring system in smart grid. *IEEE Communications Magazine, 50*(5), 142–149.
- Raza, H. (2011). A brief survey of radio access network backhaul evaluation: Part I. *IEEE Communications Magazine, 49*(6), 164–171.
- Sridharan, S., Dawson, E., & Goldberg, B. (1991). Fast fourier transform based speech encryption system. *IEEE Proceedings-I, 135*(3), 215–223.
- Su, H., Qui, M., & Wang, H. (2012). Secure wireless communication system for smart grid with rechargeable electric vehicles. *IEEE Communications Magazine, 50*(8), 62–68.
- Tamayo-Fernández, R., Mendoza-Valencia, P. J., & Serrano-Santoyo, A. (2011). An architecture for design and planning of mobile television networks. *Journal of Applied Research and Technology, 9*, 277–290.
- Tartarelli, S., d'Heureuse, N., & Nicolini, S. (2010). Lessons learned on the usage of call logs for security and management in IP telephony. *IEEE Communications Magazine, 50*(12), 76–82.
- Tribolet, J. M., Noll, P., McDermott, B. J., & Crochier, R. E. (1978). A study of complexity and quality of speech waveform coders. *IEEE International Conference on Acoustics, Speech, and Signal-Processing, ICASSP '78*, 556–590.
- Vingelmann, P., Fitzek, F. H., Pedersen, M. V., Heide, J., & Charaf, H. (2011). Synchronized multimedia streaming on the iPhone platform with network coding. *The 8th Annual IEEE Consumer Communications and Networking Conference—Multimedia & Entertainment Networking and Services, 49*(6), 126–132.
- Yasumoto, K., Nunokawa, Y., Sun, W., & Ito, M. (2011). Improving mobile terrestrial TV playback quality with cooperative streaming in MANET. *IEEE WCNC 2010—Service and application*, 2101–2106.
- Yin, P., Min, L. (2010). A color image encryption algorithm based generalized Chaos synchronization for bidirectional discrete systems for audio signal communication. *International Conference on Intelligent Control and Information Processing*, Dalian, China, (pp.443–447) August 13–15, 2010.