A Novel Chaos-Based Voice Controlled FTP Tool

Muhammed Maruf Ozturk, Akif Akgul, Sezgin Kacar

Abstract: To manage file transfer operation, various tools have been developed so far. However, these tools can not respond adequately for conduct a secure transfer. Also few works have been done using encrypted voice controlled system yet. By regarding this lack, we investigate how to built a useful and secure tool. This work presents a novel improved voice controlled FTP tool (Wb-CFTP) using chaotic system. A chaotic system called as logistic map is associated with Wb-FTP designed on the basis of Asp.Net and C#. Here we depict the prominence of encryption in voice controlled systems.

Index Terms: Chaos, Logistic map, Encryption, FTP tool, Voice recognition, Web interface, Nonlinear equations

1 Introduction

NOWADAYS, the use of FTP tools are gradually being widespread. Becoming widespread use of cloud systems require the use of FTP for personel data saving. To transfer files, first protocol was unveiled by 1976 by Michel Gien [1]. This tool has been varied through the last decades. The increase of FTP tools shows that Ftp management should be accessible and reliable for users. A voice controlled FTP tool consists of following components:

- Speech recognition engine
- Specific grammar
- An algorithm
- Voice control software.

A voice controlled FTP tool consists of a recognition algorithm, speech grammar, recognition engine, and a software which drives these components. Voice and speech recognition are terms which are commonly used interchangeably by researchers. But these notions quitely refer different operations. Voice recognition is concerned with grammar rather than pronouncing and it includes command device and recognition system. These systems fine naive human voice to produce various results. Voice recognition algorithms are of two parts. First is training phase and the second is testing [2]. In training phase, user gives sample voices to system thus system learns some voices. The level of the success of this operation is measured in testing. As we repeat words, system learns them as well. Validation is in testing that is done by matching recorded words. Voice controlled systems has long been the focus of some works. However, encrypted voice control can be considered as a new notion. In this paper, we strive to show simple steps of speech tune parts. Proposed Wb-CFTP presents an alternate method to manage FTP operation. Wb-CFTP first listens the words given to the system and then conducts FTP by using a robust encryption. This work can be evaluated in terms of file transfer that encryption is only in this part. Inputs may include some noises. There are some filtering methods to prevent skewed input. Inherently, encryption is with some problems as in other fields. Despite the powerful encryption, noise may occur. To reduce the probability of noise in input, the correctness of the data can be detected during encryption. In recent years, enhancement in digital technologies led to make more reliable communication systems [3]. It is not eligible that the advancement in micro and computer aided systems support this case. It is widely accepted that todays encryption algorithms, even the powerful ones can be cracked in a specific time [4]. The recent encryption studies emphasize that there is a high correlation between chaos and cryptology sciences due to the special properties of chaotic systems [5]. The chaotic systems have the properties of wide-band, noise-like, hard to predict and aperiodic [6]. Due to the chaotic signals show noise-like behavior and strong dependence [7] on initial values and parameters, it makes chaos based encryption more preferable for secure communication. The encrypted data include complex or noise-like feature and this is prominent for data to keep data uncracked. The paper makes following contributions: 1) A novel FTP tool; 2) Depicting the importance of chaotic encryption in FTP management; 3) Enhance the level of security for tools to be developed. The rest of paper is organized as follows: Section 2 includes a literature review. Section 3 detaily introduces mathematical background, method and chaotic system. In Section 4 obtained results and the contribution of the paper are stressed.

2 RELATED WORKS

2.1 Chaos Based Systems

Contrary to recently used standard encryption algorithms, numerous works with chaotic systems has starting increasing. Chaotic systems have become more popular in encryption as they can successfully maintain infusion and diffusion, the basic components of encryption, by providing complexity with activities like noise and being sensitive to initial conditions [8]. One of them is data that is to be hidden as into the equations in which presents in chaotic systems that will not break the chaotic behavior [9]. Another is the encryption with chaos by mixing original data and data from chaotic system [3]. There is the encryption is being performed thanks to the complexity property of Chaotic systems by making original data more ambiguous than first. In Chaos based operations to make encrypted data complex, some methods can be executed such as delaying, switching [6]. In such operations to unveil hiding data we should comprehend switching time and delaying time

- *Muhammed Maruf ÖZTÜRK, Sakarya University, Department of Computer Engineering, Faculty of Computer and Information Sciences Sakarya, TURKEY,e-mail: muhammedozturk@sakarya.edu.tr*
- *Akif AKGÜL, Sezgin KAÇAR, Sakarya University, Department of Electrical-Electronics Engineering, Faculty of Technology, Sakarya, TURKEY, e-mail: aakgul@sakarya.edu.tr, skacar@sakarya.edu.tr*

as well as the structure of encryption algorithm. Various works are performed encryption using multiple chaotic system [10]. Before the initialization of this sort of encryption, used Chaotic systems and signals that produced in Chaotic systems and the order of signals must be known together. While decrypting of data that encrypted with Chaos, a minor fault could prevent to the decryption of data. This sensitivity property is preferred in encryption works. In some works the encryption is done mixing Chaotic and Non-Chaotic methods [5]. However these encryption operations adversely affect large image and audio files in terms of speed. A safe communication is one of the most significant needs of our era. Many studies on hiding data types like text, audio, image and others have been carried out in order to meet such need. In this article, a study on increasing the security of audio data has been executed. Many studies on audio data encryption have appeared in the literature so far [8–11]. Some of these included directly hiding audio files while others included methods of hiding the information by embedding some other data in the audio files. The general objective of all these studies is to prevent the possession of data by undesired people.

2.2 Voice recognition

Speech recognition works can be examined in three categories: command controlled; command reinforcement, and control applications. Control applications are associated with the components in which voice commands are explored. In order to achieve robust systems, speech technology is used for authorization. These systems have some advantages. One of them is such systems facilitates the way of living for physically disabled people [12, 13]. Voice controlled systems including computer or electric supported devices have long been the objective of previous studies. One of them developed two voice controlled program [14]. It includes Lithuanian and English speech motors then the result of them are verified latter. An e-market application [15], which was combined with C# and .NET, presents a performance comparison to be a good example of voice controlled systems [16]. This work stresses the prominence of the use of voice control arguments in FTP operation. The differentiation of speech was also used in robot technology [18]. House et al. introduced VoiceBot and one of the results of this work is that voice controlled robots could be the leading for future works [17]. Mustaquim depicted the importance of fuzzy in voice controlled games by developing a new recognition algorithm [16]. Despite the promising results, some faults have not been removed yet in air traffic systems. This study shows that voice control augments the performance time approximately 50% for some types of tasks. Also speech recognition had been used robot technology before. In Shie and Maier's work a VoiceBot was introduced and evaluated [17]. The results of the study showed that voice controlled robotics are feasible, and portend extremely well for future research. Although the use of speech for controlling of games is not widely known, Mustaquim has developed a new algorithm [18] benefiting fuzzy logic that revealed the importance of voice support in games. Using speech commands a significant success has been obtained in the field of air traffic control [19]. Despite the promising results, specific errors has not been reduced completely yet. Butt et. al's work has stressed that a more secure voice controlled system is needed using current technologies [20-21].

2.3 Integration of Tools

MATLAB Builder NE and its Web Figure property is the basis of current applications which performed on various scientific areas. In one work completed in 2009, a web interface was developed for wireless sensor networks using MATLAB Builder NE and Web Figure [22]. In another work that released in 2010, an educational interface was designed for the teaching of digital modulation techniques [23]. These tools were also used in two different works related to biomedicine in 2011 [24, 25]. In addition these tools were used in one work including complex functions such as frequency analysis of nonlinear systems [26]. These works strongly endorse that MATLAB Builder NE and Web Figure have been efficiently used in analog communication and web based educational image processing interface that present flexible and easy usage to users [27, 28].

3 Method

The methodology used in this study has three steps. These steps has three functions, including voice recognition engine, ftp management page and encryption algorithm. While examining similar works, we have encountered similar works which present optional way to design voice recognition engine. The findings show that voice recognition engine based on .NET is more preferable than others when it comes to the integration of encryption with a web based tool. The main advantage of .NET is the compatible property that enable user to invoke required functions from MATLAB. Basically .NET provides a speech library called as SpeechLib that presents recognition engine including grammar rules. Voice commands are assigned to a value starting from 1. When the pronounced word is recognized, desired function is run according to the word value. Proposed tool has not a facility to differentiate user voice, especially focused on the management of ftp regardless of user type. Therefore we have not used neither any speech recognition algorithm such as Hidden Markov models [29], neural networks nor any others. MATLibrary provides integration between .NET and MATLAB, thus recognized command can be encrypted and sent back to tool. Commands are taken as .wav file that facilitates sending operation. Thanks to this function the system becomes more reliable after the encryption. Recent years Chaos is the leading method for encryption that gradually becoming popular in several areas including electric, electronic, computation and the others. Also chaos has been used in this study for the encryption of commands through the execution of system functions. Voice commands are transformed to byte arrays than sent to the encryption algorithm. Thus, designed system's robustness and reliability are dramatically improved. The overview of the model is shown in Fig. 1.

3.1 The Need of Encryption

Although FTP is a widely used protocol, it has still some vulnerabilities. The security requirements are gradually increasing as the way of data transfer is changing. Various tools provide a few encryption rule such as AES, Blowfish, Cast5, DES and RSA. This brings a secure layer that hardens ftp operation. It is desired that security should not significantly effect the efficiency of data transition. To reach a sufficient efficiency, design of data channels is hard to built when it is compared to other factors [30]. While designing of server we should consider key points such as IP access, resource access control and connection limitations. It is clear that flexible, secure and efficient data transfer is possible by using new integration and encryption methods

3.2 Chaos Based Encryption

A non-linear equation is used in order to increase security in encryption. One needs to know b parameters and what kind of equation is used in order to decrypt data encrypted with the function in Equation 1. "x" value in the function represents the keys produced with chaos generators and "m" value that represents the audio data to be encrypted in bits [2].

$$f(x,m)=(2x(1+xm+1-m)+a)/b \qquad (1)$$

In this study, parameters (a,b) are selected respectively as 0.9, 0.8. Choosing an appropriate value range for equation and parameters is necessary to achieve a chaos based encryption. When certain limits are exceeded, the system gives up the use of chaos and thus chaos based encryption is not completed. Fig. 2 exhibits the general block diagram of encryption application for safe transmission of any audio data. As can be seen on the block diagram, audio data and keys produced with chaotic systems are encrypted with the help of a function. Aftermath encrypted data seen later in the block diagram can be decrypted with the inverse of the function. In order to decrypt audio data encrypted in the application in this figure, one needs to know keys produced for each bit and the order of these keys, the chaotic system used, parameters in the chaotic system and initial values, and also non-linear equation and all parameters employed in this equation. Otherwise, it is not possible to decrypt the encrypted data.

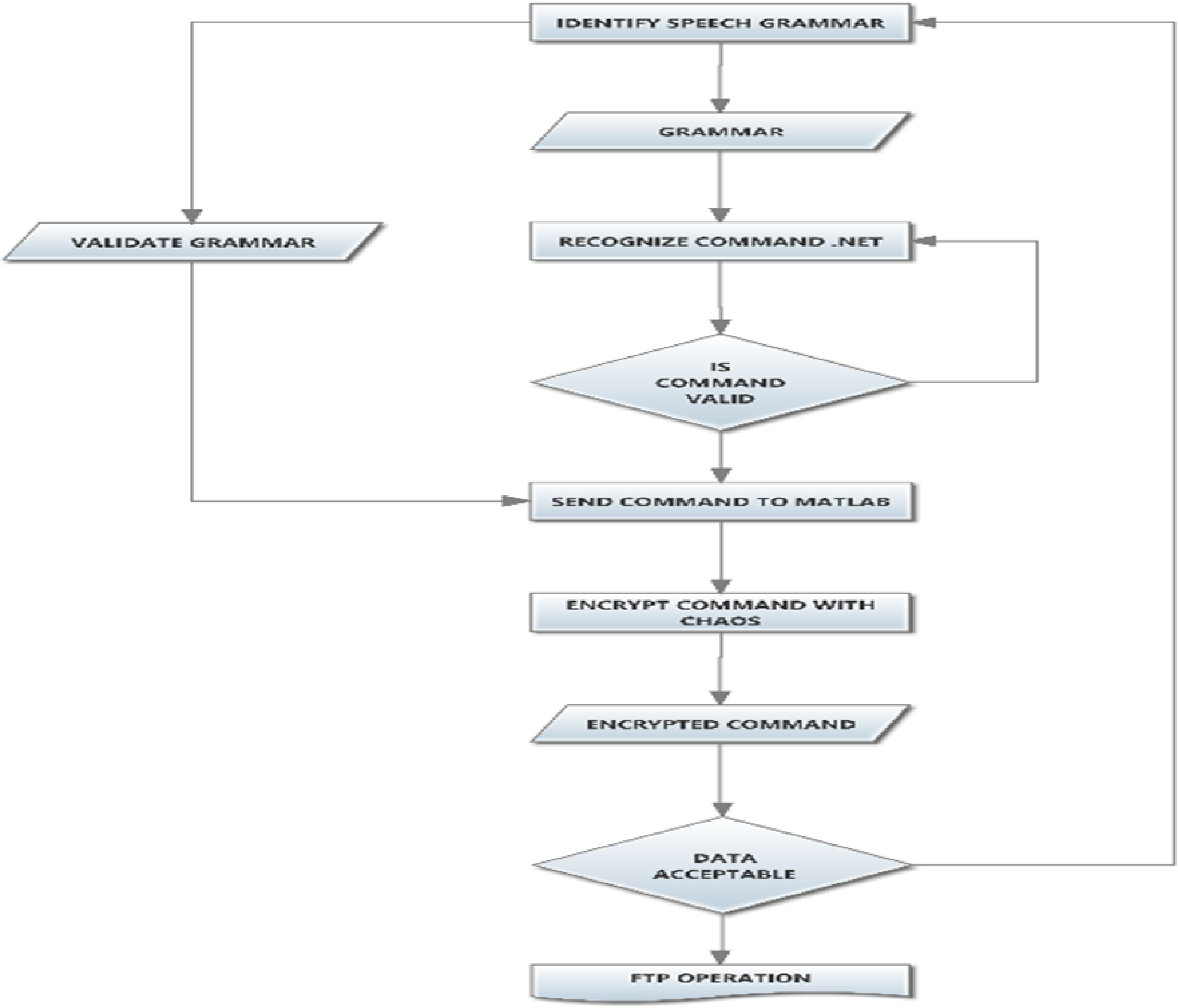


Fig. 1. *The overview of presented model*

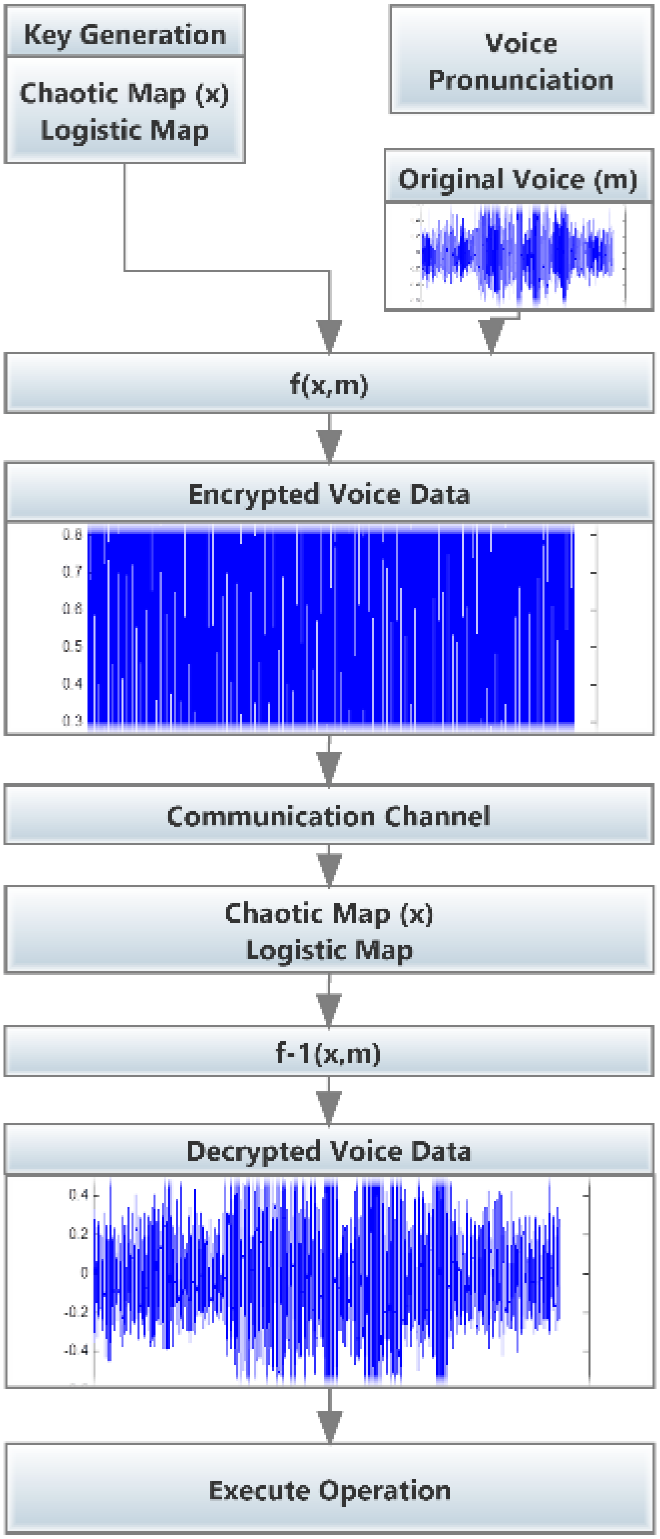


Fig. 2. *Block diagram of encryption and decryption of audio data*

3.3 Discrete-Time Chaotic Systems Used in Encryption Application

Logistic Map (Equation 2) is a commonly used single dimension chaotic system. Fig. 3 exhibits bifurcation diagram shows that which intervals are seen while Logistic Map is entering to the Chaos. 'r' parameter is examined between 0-4 values. Bifurcation diagram in Fig. 3 shows that r value must be chosen 3.5699-4 so that the system can enter chaos. Otherwise, the system does not enter chaos and keys which necessary for encryption are not produced thus chaotic encryption is not be possible [1].

$$X_{n+1} = r * X_n * (1 - X_n) \qquad (2)$$

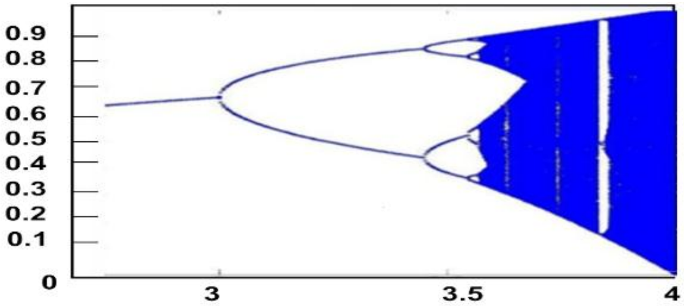


Fig. 3. *Logistic map bifurcation diagram*

'X' value represents the system variable, and r represents the system parameter in Equation 2. n value is changeable according to the data to be encrypted. Value of n depends on how many bits of data will be encrypted.

3.4 Implementation

Initially, a user friendly web interface is designed. This design, including manual or voice enabled controlling, is differ in terms of usage and robustness when it is compared with other available tools. Traditional tools are developed to only manage ftp operation regardless of command transition security. But nowadays network tracking methods are dramatically increased thus communication should be covered with new techniques. Designed tool interface is shown in Fig. 4. T1 is the pre-operation time that should be less than 10 seconds. If an over waiting time is determined, recognition engine is temporarily suspended. P1 is to represent the operation and saved to L1. The most used commands transferred to Lk from L1. This reduces operation time significantly that the steps shown below.

- Start speech recognition engine and record time at T1
- Save the frequent Wb-FTP operations on P1
- If T1>10 seconds than disable speech recognition engine.
- Save P1 operation list into database and select frequent list as follows:
  - insert into L1(op1,op2,...) values(P1)
  - select P1.op1, P2.op2., ..., Pk from L1
- Save the frequent Wb-FTP operations in Lk.
- Operate Lk and P1

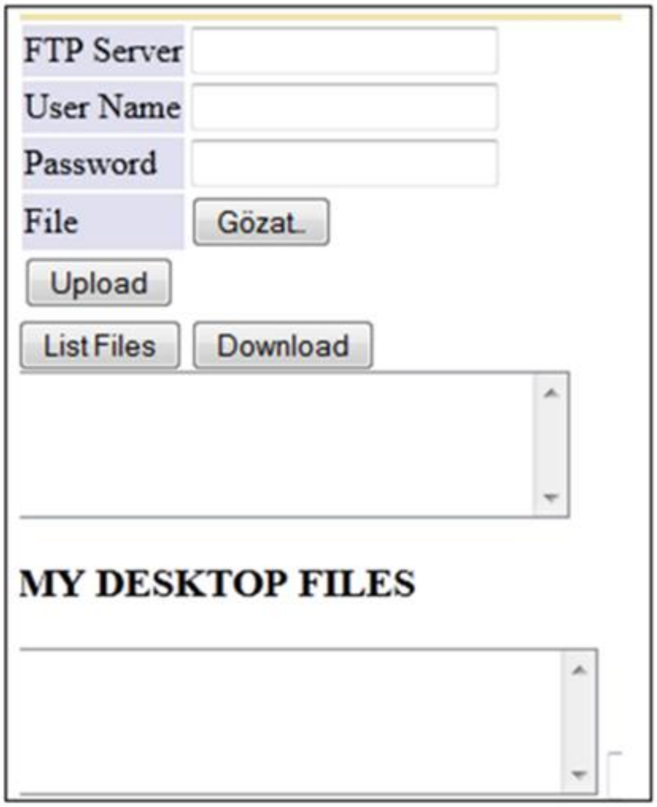
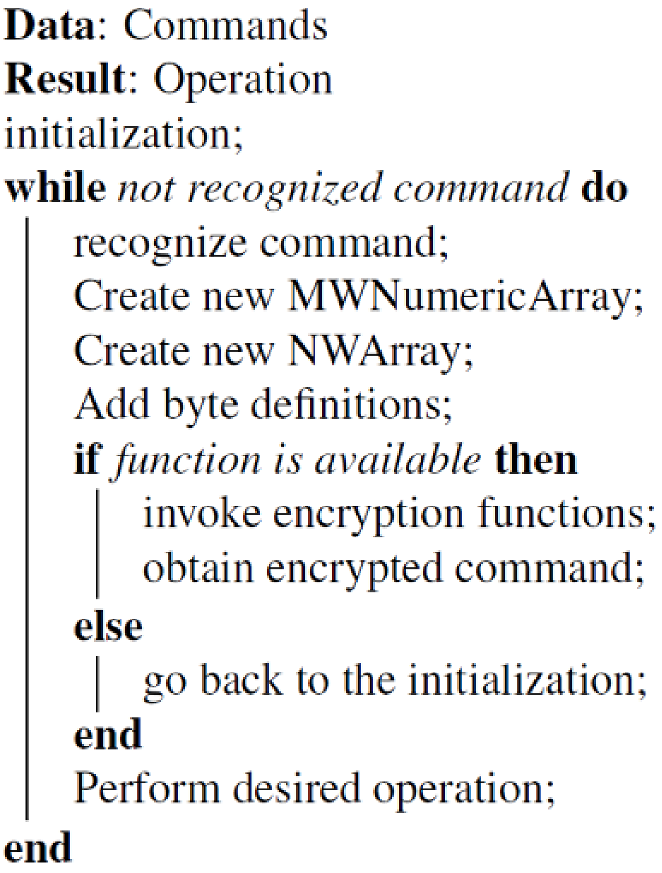


***Fig. 4**. Web interface*

Operations shown above are respectively executed. After the completion of the operations, encryption algorithm is applied to recognized command. To implement the encryption a suitable encryption algorithm has been designed. In the algorithm, initially required array definitions are specified to be filled with voice command. Aftermath the path of command is assigned to new path that will be used as the encryption way. There is a connection between MATLAB and .Net framework that provides an encryption method which takes information from .Net interface and delivers to the encryption function. The function is available in a class that can be extended adding new functions. To illustrate encrypted and decrypted commands three WebFigure objects have been used in developed tool. These objects are filled with encrypted bytes. Designed algorithm is shown in Algorithm 1. Fig. 5, Fig. 6, Fig. 7 respectively show the original, encrypted and decrypted voice command. As shown from the Fig. 5 and Fig. 6 encrypted command data present similar distribution that complicates the decryption of encrypted command.

Algorithm 1. Web interface



```
Data: Commands
Result: Operation
initialization;
while not recognized command do
    recognize command;
    Create new MWNumericArray;
    Create new NWArray;
    Add byte definitions;
    if function is available then
        invoke encryption functions;
        obtain encrypted command;
    else
        go back to the initialization;
    end
    Perform desired operation;
end
```

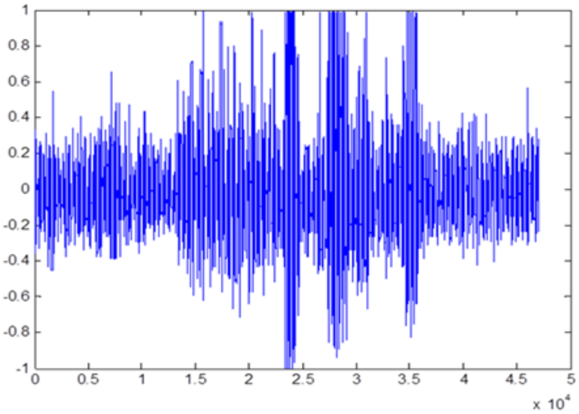


***Fig. 5.** Recognized command*

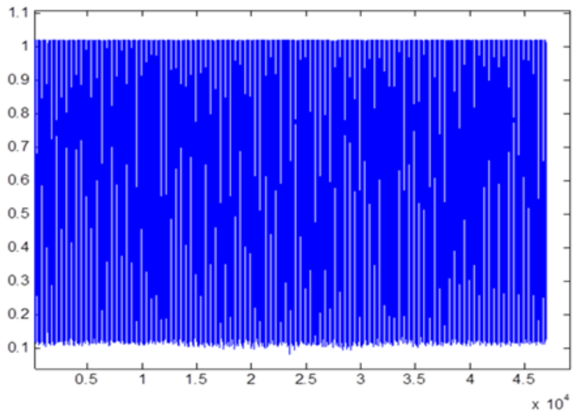


***Fig. 6.** Encrypted command*

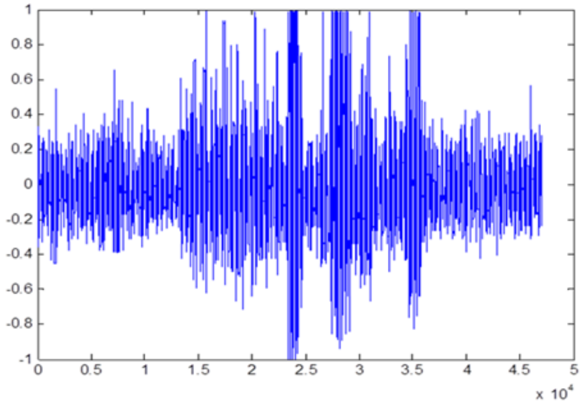


Fig. 7. *Decrypted command*

4 Conclusions and Future Work

Encryption is required when a reliable data transition is desired. Here we propose an encrypted voice controlled ftp tool. Using encryption a reliable and robust tool has been obtained in terms of communication. On the other hand designed tool has a user friendly interface that easily realized while performing ftp operations. Main contribution of the work is the involvement of chaos based encryption in ftp operation. With respect to the encryption, proposed tool could shed new light for voice controlled systems. One threat that encountered while developing is the security level of encrypted system. Encrypted system has not been tested yet using any attack that causes an ambiguous security level. For further investigation security level should be taken into account that this may constitutes one aspect of the future works. Another direction, that needs to be further investigation, is the effect of various protocols such as UDP, TCP and the others in command transition. Chiefly development tools are Visual Studio and MATLAB. A well designed integration such this work produces multi-functional and robust software. If the development and the encryption can be done in one IDE, operational times could be reduced. In this point of view we have written and invoked required encryption functions from MATLAB that would have been given up if all operations were done using .Net framework. Chaos based encryption is possible using various methods. We used nonlinear equation in Chaos based encryption. The contribution of this method is adding new function to encryption that hardens the decryption of the command. Because to decrypt the encrypted command, nonlinear equation and its parameters must be known prior to the operation. Furthermore the known of the first key, which used while encryption is being done, is sufficient to decrypt the encrypted command. Other keys are produced by inversing nonlinear equation that used for encryption. Thus we can say that our proposed method is reduced process overload in memory. This advantage leads new improvement in real time applications such as microcontroller.

References

[1] M. Gien, “A file transfer protocol,” Computer Networks, vol. 2, pp. 312-319, 1978.

[2] L. Muda, B. Mumtaj, I. Elamvazuthi, “Voice recognition algorithms using mel frequency cepstral coefficient and dynamic time warping techniques,” arXiv preprint arXiv:1003.4083, 2010.

[3] Z. Lin, S. Yu, J. Lu, S. Cai, G. Chen, "Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system", Circuits and Systems for Video Technology, IEEE Transactions on, vol. 25, no. 7, pp. 1203-1216, 2015.

[4] JM. Amigo, L. Kocarev, J. Szczepanski, “Theory and practice of chaotic cryptography,” Physics Letters A, vol. 366, pp. 211-216, 2007.

[5] F. Yuan, GY. Wang, BZ. Cai, "Android SMS en- cryption system based on chaos", IEEE 16th International Conference on Communication Technology (ICCT), pp. 856-862, 2015.

[6] V. T. Pham, S. Vaidyanathan, C. K. Volos, S. Jafari, "Hidden attractors in a chaotic system with an exponential nonlinear term", The European Physical Journal Special Topics, vol. 224, no. 8, pp. 1507-1517, 2015.

[7] S. Lian, "Efficient image or video encryption based on spatiotemporal chaos system," Chaos Solitons and Fractals, vol. 40, pp. 2509-2519, 2009.

[8] B. Norouzi, S. Mirzakuchaki, SM. Seyedzadeh, MR. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," Multimedia tools and applications, vol. 71, no. 3, pp. 1469-1497, 2014.

[9] L. Teng, H.H. Iu, X. Wang, X. Wang, "Chaotic be- havior in fractional-order memristor-based simplest chaotic circuit using fourth degree polynomial," Nonlinear Dynamics, vol. 77, no. 1-2, pp. 231-241, 2014.

[10] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, "An efficient method for the construction of block cipher with multi-chaotic systems," Nonlinear Dynamics, vol. 71, no. 3, pp. 489-492, 2013.

[11] G.Troullinos, “A software based approach to secure voice applications," Proceedings of the Third IEEE International Conference on Electronics, pp. 176-182, Rodos, Greece, 1996.

[12] CH. Wang, MW. Li, W. Liao, “A distributed key-changing mechanism for secure voice,” IEEE International Conference on Multimedia and Expo., pp. 895-898, Beijing, China, 2007.

[13] K. Christian, “A comparison of voice controlled and mouse controlled web browsing”. Proceedings of the Fourth International ACM Conference on Assistive Technologies, pp. 72-79, Arlington, USA, 2000.

[14] MS. Hawley, P. Enderby, P. Green, SP. Cunningham, S. Brownsell, J. Carmichael, M. Parker, A. Hatzis, P. O’Neill, R. Palmer, “A speech-controlled environmental control system for people with severe dysarthria,” Medical Engineering Physics, vol. 29, pp. 586-593, 2007.

[15] H. Shi, A. Maier “Speech-enabled windows application using Microsoft SAPI,” International Journal of Computer Science and Network Security, vol. 6, pp. 33-37, 2006.

[16] MM. Mustaquim, “Automatic speech recognition an approach for designing inclusive games,” Multimedia Tools and Applications, vol. 66, pp. 131-146, 2013.

[17] B. House, J. Malkin, JA. Bilmes, “The voicebot: a voice controlled robot arm”. Proceedings of CHI, ACM Conference on Human Factors in Computing Systems, pp. 1-10, Boston, USA, 2009.

[18] A. Rudionis, K. Ratkeviius, T. Dumbliauskas, V. Rudionis, “Control of computer and electric devices by voice”. Elektronika Ir Elektrotechnika, vol. 6, pp. 11-16, 2008,.

[19] J. Ferreiros, JM. Pardo, R. de Córdoba, J. Macias-Guarasa, J.M. Montero, F. Fernández, V. Sama, L.F. d’Haro, G. González, “A speech interface for air traffic control terminals,” Aerospace Science and Technology, vol. 21, pp. 7-15, 2012.

[20] G. Cattaneo, L. Catuogno, F. Petagna, G. Roscigno, "Reliable Voice-based Transactions over VoIP Communications", Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 101-108, 2015.

[21] A. Akgul, S. Kacar, I. Pehlivan, "An audio data encryption with single and double dimension discrete-Time chaotic systems“, Online J. Sci. Technol., vol. 5, no. 3, pp. 14-23, 2015.

[22] D. Bansal, M. Khan, AK. Salhan, "A computer based wireless system for online acquisition, monitoring and digital processing of ECG waveforms," Computers in biology and medicine, vol. 39, no.4, pp. 361-367, 2009.

[23] QI. Ali, A. Abdulmaowjod, HM. Mohammed, "Sim- ulation & performance study of wireless sensor network (WSN) using MATLAB," Energy, Power and Control (EPC-IQ), pp. 307-314, 2010.

[24] I. Silva, GB. Moody, "An open-source toolbox for analysing and processing PhysioNet databases in MAT-LAB and Octave," Journal of Open Research Software, vol. 2, no. 1, 2014.

[25] EP. Larsen, R. Perez-Castillejos, "MATLAB interface for portable microelectrode impedance measurements," Biomedical Engineering Conference (NEBEC), 41st Annual Northeast, pp. 1-2, 2015.

[26] B. Morini, M. Porcelli, "TRESNEI, a Matlab trust-region solver for systems of nonlinear equalities and inequalities," Computational Optimization and Applications, vol. 51, no. 1, pp. 27- 49, 2012.

[27] N. Boumal, B. Mishra, P.A. Absil, R. Sepulchre, "Manopt, a Matlab toolbox for optimization on manifolds," The Journal of Machine Learning Research, vol. 15, no. 1, pp. 1455-1459, 2014.

[28] S. Kacar, C. Bayilmis, “A web-based educational interface for an analog communication course based on MATLAB builder NE with web figures,” IEEE Transactions on Education, vol. 56, pp. 346-354, 2013.

[29] K. Tokuda, Y. Nankaku, T. Toda, H. Zen, J. Yamagishi, K. Oura, "Speech synthesis based on hidden Markov models," Proceedings of the IEEE, vol. 101, no.5, pp. 1234-1252, 2013.

[30] L. Xia, F. Chao-sheng, Y. Ding, W. Can, “Design of secure FTP system,” Communications, Circuits and Systems, International Conference on IEEE, pp. 270-273, Sichuan, China, 2010.