Watermark with Fast Encryption for FPGA Based Secured Realtime Speech Communication

Hussain Mohammed Dipu Kabir[1], Saeed Anwar[2],
Abu Shahadat Md. Ibrahim[3], Md. Liakot Ali[4], Md. Abdul Matin[5]
[1]Samsung Bangladesh R&D Center, Dhaka, Bangladesh
[2]The University of Akron, Akron, Ohio, USA
[3]University of Dhaka, Dhaka, Bangladesh
[4]Institute of Information and Communication Technology
[5]Department of Electrical and Electronics Engineering
Bangladesh University of Engineering & Technology, Dhaka, Bangladesh
[1] dipu.kabir@samsung.com; [1]dipuk0506@gmail.com; [5]amatin@eee.buet.ac.bd

Abstract- **This paper presents a Field-Programmable Gate Array (FPGA) based secured speech communication system. Data-size is one of the major concerns of cryptographic systems. To maintain same data-rate compression is performed at first. Compression reduced data-size. Watermark and random key is embedded at the vacant places. There are many encryption techniques, but for realtime encryption, fast encryption is needed. FPGA is an efficient device for these operations on realtime signals. Conventional processors contain small number of registers and perform large operations in multiple cycles. FPGA can perform a large number of operations concurrently. Change has brought at the generation of random numbers. To generate more secured random number, nibble bit of noise signal is Xored with hardware-generated random number. In proposed method voice signal is compressed, watermarked, encrypted and sent through a transmission medium from the transmitting end. Receiver receives that signal and decrypts both signal and watermark.**

Keywords- FPGA; Watermarking; Compression; AES; DES; Eavesdropping

I INTRODUCTION

Digital watermarking is the technique of inserting specific information into signal, data, image or video. The specific information is known as watermark and usually used for ownership identification, authentication purpose and protection of integrity of data. Due to rapid progress in wireless communication systems, extreme prevalence mobile systems, and smart card technology, information is more vulnerable to abuse. For these reasons, it is important to make information systems secure to protect data and resources from malicious acts.

The watermark is extracted or detected at any point where identification or integrity is concerned. Traditional digital watermarking schemes are mainly based on spatial-domain or transform-domain, such as discrete cosine transform and discrete wavelet transform. In [1] Z. M. Lu, et al. proposed a novel Vector Quantization (VQ)-based watermarking algorithm. An electronic identification control of consumer electronics creates a unique security code, based on user's information and user's security code [2]. The smart card-based scheme is a very promising and practical solution to remote authentication. Compared with other smart card-based schemes, our solution achieves more functionality and requires much less computational cost [3]. Health information of individuals is important for improving patient's safety and quality of life [4]. That information should be transmitted in a secured channel or in an encrypted way. Hardware based security systems are more robust [5]. The generation of encryption secret keys with a high level of security is crucial to ensure secure enduring data storage and is a challenging topic of investigation [6]. We need to improve our administration. While technology has changed the world administration and education of under-developed countries are ineffective. Secured technology is required for administrations [7]. Mobile banking has becoming common in developing and overpopulated countries, such as India and Bangladesh. This increasing use faces some security challenge [8]. Trust and security issues of mobile banking are also important for developing countries [9].

Robust, fragile and semi-fragile approaches [10], [11] are the classification of recent watermarking techniques. The robust watermarking approach protects the copyright identifier of data in which watermarks are not easily removed by attacks. The fragile watermarking approach confirms content integrity. However, speech, a one-dimension signal, victim of replacement attacks, such as copy-and-paste, counterfeiting and transplantation attacks, and deletion and insertion attacks that manipulate speech length. The proposed algorithm can overcome these problems. As encryption system is concatenated with it watermarking attacks are not yet powerful. In case of copy-paste, cropping, shifting original signal and watermark becomes protected. In case of counterfeiting original signal is damaged, if it is tried after encryption; so none will do it. Recently watermark is also used for quality evaluation of speech [12].

Conventional watermarking algorithms have been developed for software implementations due to ease of use, upgrading opportunity and flexibility. However, the software implementations have the limitation of speed and are vulnerable to the off-line attacks. The high density techniques of current FPGAs will be a highly attractive solution for hardware implementation of the software-based watermarking algorithm as they provide flexibility, easy implementation and high performance [13-16].

Encryption is necessary to ensure protection of data in the medium. Traditional symmetric key encryption algorithms like Data Encryption Standard (DES) use small blocks size with complex permutations process to give secure output cipher text [21]. Public key algorithms are not suitable for large amount of data due to its slow performance [17-18]. Advanced Encryption Standard (AES) was announced by National Institute of Standards and Technology (NIST) on 2001. AES is one of the most secure algorithms used in symmetric key cryptography [19-20]. It uses complicate repeated steps to prevent analytic attacks that can discover weakness in the algorithm and so attack any encrypted data. AES use high diffusion to eliminate any prediction of key. The only problem with AES is its sensitivity to noise due to its high diffusion. The diffusion make elements within each block depend on each other (mix-column step). So if one element or more missed or corrupted by noise it will affect the surrounding elements and the error will propagates and increase in next round. Therefore the AES problem may appear in noisy channels only because of repeated rounds that cause propagation of error. Decreasing number of rounds or cancel mix column step will affect the security of algorithm so solution will be depend on other security aspects to protect algorithm when decreasing diffusion.

In this paper, a FPGA implementation of compression, watermarking and encryption algorithm over speech signal is presented. The algorithm for decryption, identification or authentication and reconstruction of original signal is also represented. Compression is needed to prevent the increase of the data in transmission channel. Encryption provides security while the signal traveling via the transmission channel. Encryption is performed using random number and secret keys. So, it is very difficult to decrypt this without knowing the algorithm. In FPGA based encryption system, random number is generated by XORing the nibble bit of a noise with a clock. Frequency of this clock is higher and not an integer multiple sampling frequency. Nibble bit of any noise signal is almost a random number. XORing with this clock resultant will be another random number. Purpose of taking nibble bit of noise and high frequency clock is to avoid random sequence.

In compression part of proposed system, non-linear down-sampling compression technique [22] is used; which is a lossy compression technique. Loss-less compression technique may also be used [23]. For low-frequency signal, original signal can be recovered with little noise, but for high-frequency input signal interpolation reconstruction is not enough.

II MATHEMATICAL BACKGROUND

A. Down-sampling for Compression

In 1.5 factor non-linear down-sampling technique, one sample is discarded after taking two samples. When the frequency of the main signal is small compared to Fs, main signal can be reconstructed from down sampling data with very small noise. At high frequency, two noise signals are found. As it is nonlinear down sampling, original signal with slightly smaller amplitude is found because of one same sampling period and also obtaining noise of folding frequency, $F = (2/3)F_N$ because of one double sampling period. Amplitude of noise is equal to amplitude-difference of original signals [22].

Let, F_s = Sampling Frequency
F_N = Nyquist Frequency = $F_s/2$
n = sample number = 1, 2, 3, …
Let us assume a signal of frequency, $F= (2/3) F_N+f_1$ Hz

$$f = \frac{2}{3}F_N + f1Hz \quad (1)$$

So, Folded signal,

$$S_f = sin(2\pi\frac{(\frac{2}{3}f_N - f1)n}{F_s}) = sin(2\pi\frac{n}{3} - 2\pi\frac{f1n}{F_s}) \quad (2)$$

[As, $Fs = 2 * F_N$]
Original signal,

$$S_m = sin(2\pi\frac{(\frac{2}{3}f_N + f1)n}{F_s}) = sin(2\pi\frac{n}{3} + 2\pi\frac{f1n}{F_s}) \quad (3)$$

From eqn. (2) and eqn. (3), a relation between these two signals is found. That is-
Folded signal - Original signal $= S_f - S_m =$

$$sin(2\pi\frac{n}{3} - 2\pi\frac{f1n}{F_s}) - sin(2\pi\frac{n}{3} + 2\pi\frac{f1n}{F_s}) = \quad (4)$$

$$-2\ cos(2\pi\tfrac{n}{3})sin(2\pi\tfrac{f1n}{F_s})$$

Here, $sin(2\pi f1n/F_s)$ is the low frequency noise signal,
S_1; it's coefficient, $-2cos(2\pi n/3) = 1$ for $n\%3 = 1,2$.
Also, $-2\ cos(2\pi n/3) = -2$ for $n\%3 = 0$.
So, for consecutive 2 samples,
Folded signal - Main signal = Low frequency noise signal.
This relation is not true for discarded third sample and this causes noise.

According to this relation, some part of main signal may create noise and folded signal and low frequency noise signal are of same amplitude. Low frequency signal can be extracted using filter and shift it by $(2/3)F_s$ and then subtracting with entire signal, folding noise can be eliminated. Low frequency noise is eliminated using a low-pass filter. Compression is the first step of encoding and also the last step of decoding at the receiver end.

B. Watermark

Watermark can be any identifying sequence or copyright mark. For IP-phone, the watermark may identify the device MAC or IP address or both for proper identification. Copyright information can represent any enterprise or organization.

C. Encryption

In the proposed system, encryption is performed with successive XORing operation. From the property of XOR operation given in Eqn. (5), the encryption and decryption operation is performed.

$$(S \oplus R) \oplus R = S \quad (5)$$

Where, S represents sampled signal sequence and R represents random number sequence and $\oplus$ denotes Xor operation.

III PROCESS FLOW

Audio signal compressed, watermarked and encrypted before sending. At the primitive stage of compression, audio signal is divided into frames. A number of samples of speech signal create a frame. Frame of 15 samples is considered. Through this arrangement, proposed encryption technique will also be applicable for 30, 45, 60… sample-containing frames.

In proposed method programmed FPGA chip is used. Fig. 1 shows the arrangement for encryption in FPGA1 and Fig. 2 shows the arrangement for decryption in FPGA2.

Mod-15 counters are implemented inside FPGA of receiving-end by Verilog coding. Standard counter code (Available in internet) is used. Counter starts from 1 and its reset value is also 1. Reset is performed at the start and when the value of the counter is 16.

According to Fig. 1, sampled voice signal is received synchronously using the CLK used for sampling. When 15 samples of a frame are received, watermark and encryption starts.

A. Compression

To compress the speech signal, non-linear down-sampling process is used. In this process, mid sample of every three successive samples are dropped and available space is created. For example, consider the system shown in Fig. 1. The input consists of the fifteen samples s1, s2, s3, s4, s5, s6, s7, s8, s9, s10, s11, s12, s13, s14, s15 shown in Fig. 3. The output set will be s1, s3, s4, s6, s7, s9, s10, s12, s13, s15 (10 samples). That means samples- s2, s5, s8, s11 and s14 are discarded. After that all samples will be shifted towards left. That means 10 samples will occupy 10 leftmost spaces. 11th and 12th places will contain two watermark- w1, w2 and 13th-15th places will contain three random numbers- r1, r2 and r3.

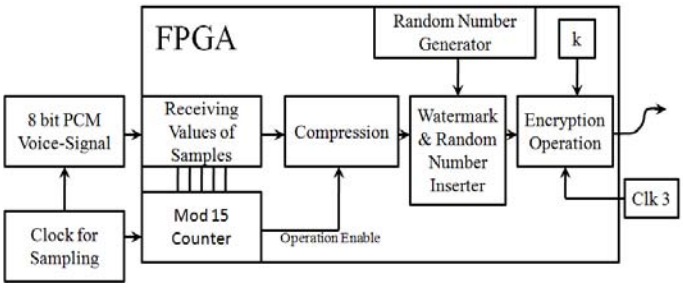

Fig. 1 Arrangement for transmitting the speech signal in FPGA

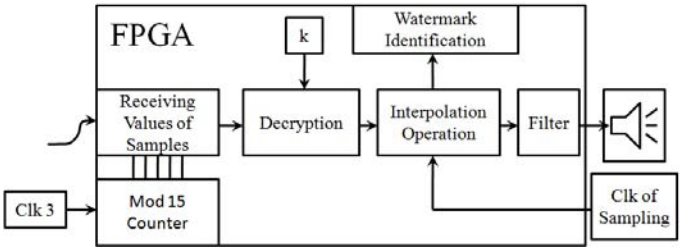

Fig. 2 Arrangement for receiving the speech signal in FPGA

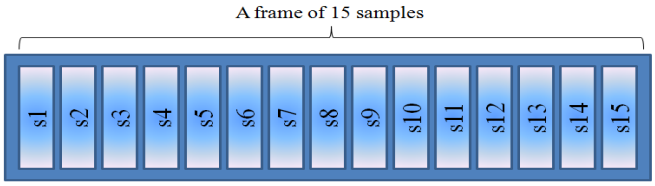

Fig. 3 A frame of 15 samples

During reconstruction at the receiving end, higher order interpolation reconstruction technique is used to reconstruct the dropped samples s2, s5, s8, s11, s14. If the frequency of the main signal is small compared to the sampling frequency Fs, then the main signal can be easily reconstructed with a little noise through interpolation technique. When frequency of input signal is high, non-linear down-sampling interpolation can be used.

B. Watermarking

After compression, spaces are evolved for watermark. If 15 successive speech samples are considered, then after compression, 5 samples are freed in each packet in which two samples are used for watermark. The frame size is not changed and the watermark signal is buried between the voice samples and random number bits. So, it is difficult to identify the watermark in the signal.

The watermark signal may be device identifier code like Media Access Control (MAC) address, International Mobile Equipment Identity (IMEI) number, Internet Protocol (IP) address or any copyright information. The watermark is placed in 11th and 12th sample position of the 15 sample frame. So the watermark is buried in the frame which is not easily detectable. The watermark signal is available in every successive 15 samples. So, in case of any cropping or any other operation is performed on signal, the watermark signal is still available.

C. Encryption

After inserting the watermark signal, random bytes are concatenated. They are marked as r1, r2 and r3. During generation of random bytes, nibble bit of noise signal is used. At first random number is obtained from a source/ hardware block. All natural random numbers are periodic, thus they are predictable when one period is observed. Nibble bit of noise is Xor-ed with this random number to increase the degree of randomness. The random number is used to encrypt the signal. The first step is to randomize the signal. Firstly, the frame of 15 samples is divided into Block A, B, C, D and E shown in Fig. 4. The first step is given in Eqns. (6) - (9).

$$A = A \oplus E \quad (6)$$
$$B = B \oplus E \quad (7)$$
$$C = C \oplus E \quad (8)$$
$$D = D \oplus E \quad (9)$$

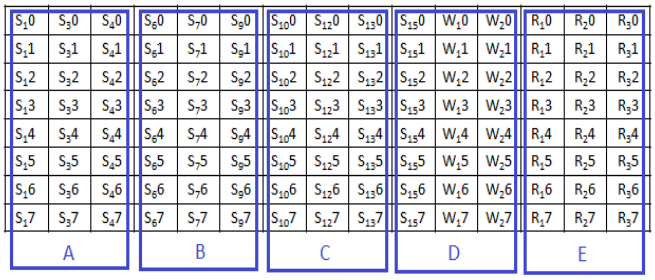

Fig. 4 The frame with block A, B, C, D and E

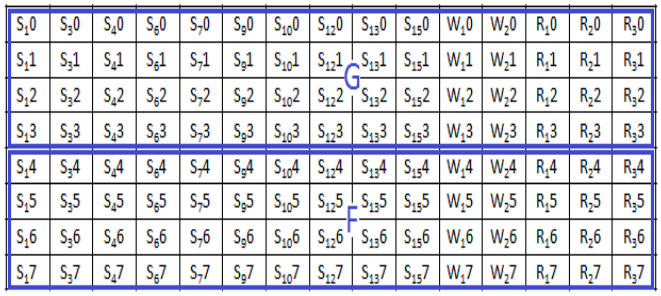

Fig. 5 The frame with block G and F

The next step is to XOR the signal again 8 X 15 bit secret key (K) given in Eqn. (10). This secret key is available at both transmitting and receiving end.

$$Signal\_Frame = Signal\_Frame \oplus K \quad (10)$$

Then the signal is made more randomised using the operations given in Eqns. (11) - (12). The F and G block defined in the frame is shown in Fig. 5.

$$F = F \oplus G \quad (11)$$
$$G = G \oplus flip(F) \quad (12)$$

In the next step, the operations of Eqns. (13) - (15) are executed.

$$A = A \oplus C \oplus D \quad (13)$$
$$B = B \oplus D \quad (14)$$
$$E = E \oplus C \oplus D \quad (15)$$

And in final step of encryption is given in Eqns. (16) - (17).

$$C = C \oplus B \quad (16)$$
$$D = D \oplus A \oplus B \quad (17)$$

The above two steps (Eqns. (13) - (17)) provides more security of the frame while transmitting in the media. The proper decryption is possible only when correct sequence of operation and block selections are known properly. FPGA will perform entire encryption steps in one positive edge of clock and within 5ns according to wave-shape editor of 'Quartus II' software. FPGA can perform a lot of task in parallel. Some Large FPGA contains billions of registers and gates. FPGA is configured according to Verilog, VHDL, System-C during program-write stage. When the FPGA is programmed it can execute a large number of instructions within a few nanoseconds [24] as it performs parallel operation.

D. Transmission

Clock 3 (External Clock) is used for transmitting signal. Here, the transmission media used is lossless wire media. In practical both wired and wireless media can be used for transmitting signal. The medium is expected to be high bandwidth and high Quality of Service (QoS). But there may be possibility of alternation of data during transmission. The altered frames are dropped during Frame Check Sequence (FCS). As the communication scheme is concerning about voice, so User Datagram Protocol (UDP) protocol is preferable.

E. Decryption

As random signal is used for encryption and that random signal is also encrypted, encrypted random signal should be sent with original samples.

At the receiving end, decryption operation is performed. The decryption process is just the reverse order of sequences of encryption process. So, the decryption sequence for our scheme is given below which starts with Eqn. (17) and reversely ends with Eqn. (6).

As any alternation of the frame in the transmission media is completely unpredictable, so recovery from that is impossible. Only possible thing is to detect the change in the frame using checksum and parity bits. The corrupted frame is eventually discarded.

F. Reconstruction

During compression, some samples are dropped. Here, s2, s5, s8, s11, s14 from the successive 15 samples are dropped. These signals should be reconstructed. As the middle bit of every 3 bit is dropped, so reconstruction is quite efficient. Here, higher order interpolation technique is used for signal reconstruction. In case of high frequency signal noise elimination is needed after interpolation reconstruction

according to ``Mathematical Background'' section. FPGA chip can handle such operation with great performance. Finally, a speaker is used which transforms the electrical signal to audible sound wave.

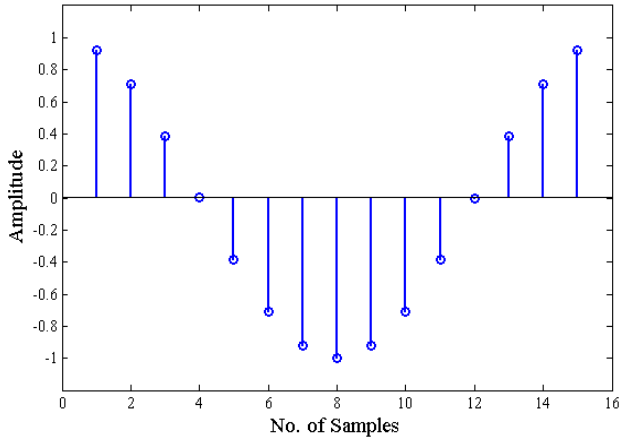

Fig. 6 Original Signal, sine wave (considered)

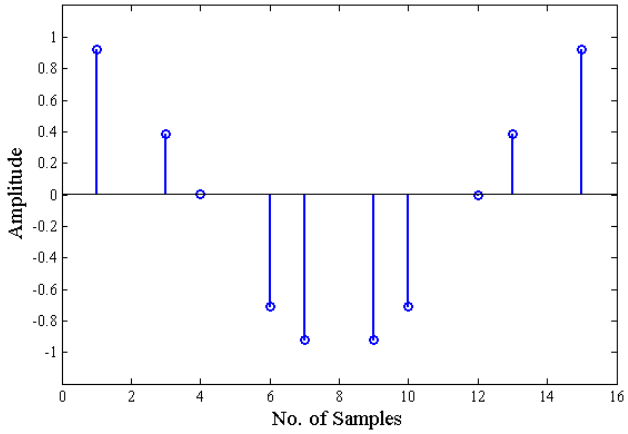

Fig. 7 After Non-linear down sampling operation

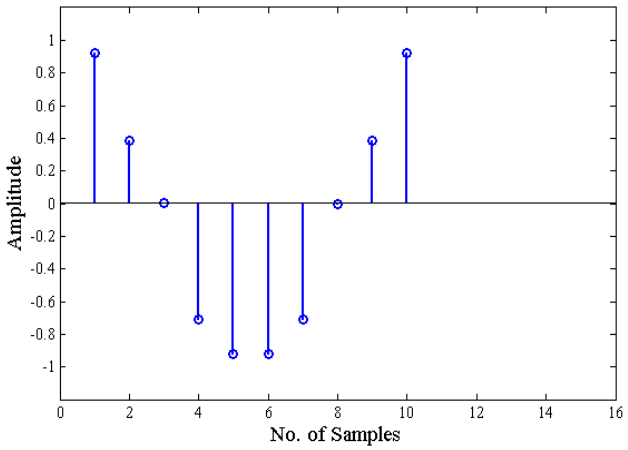

Fig. 8 Compressed signal, after down-sampling

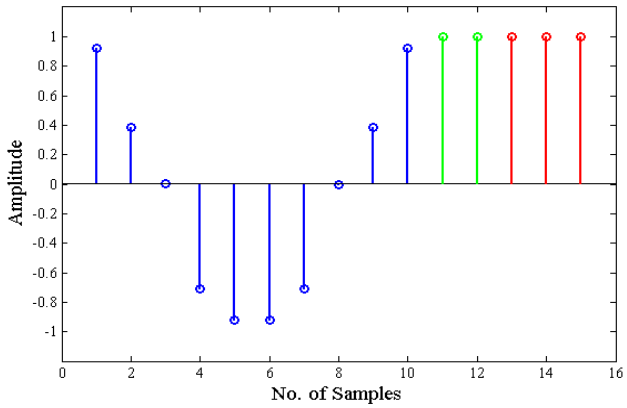

Fig. 9 Watermark (Green) and random samples (Red) are concatenated into compressed signal

IV RESULT

In proposed system, frame-wise operations will be preformed. Realtime operation of compression, encryption and watermark is performed using FPGA. To see the entire wave-shape of encrypted and watermarked signal simulation is performed using Matlab. The technique is verified for 5 male, 5 female voice signals.

A. Compression, Watermark, Encryption and Decryption of a Single Frame

For encryption of a single frame a pure sine wave is considered as original signal for better realization. Original signal is shown in Fig. 6. The compressed signal of Fig. 8 is found after down-sampling at Fig.7 and compressing. Finally the watermark and random number sequence are inserted and the final frame is shown in Fig. 9. In Fig. 9 green stems are watermark information and red stems are random numbers. Watermark signals are sent periodically. Such as three watermark information w_1, w_2, w_3, exist. We will sent w_1, w_2 with Frame 1, w_3, w_1 with Frame 2, w_2, w_3 with Frame 3 and again w_1, w_2 with Frame 4.

B. Compression, Watermark, Encryption and Decryption of entire voice signal

For simulation five male, five female, sound of bird and sound of train is used. Encryption-decryption with watermark is reversible one to one system. For compression some loss of information occurs. For low frequency sound this loss is negligible. Speech signal is of much low frequency and can be reconstructed easily using interpolation. Fig. 10 shows a speech signal. This signal is watermarked and encrypted in Fig. 11. Watermarked and encrypted signal varies from simulation to simulation for same input signal because random numbers are used for encryption.

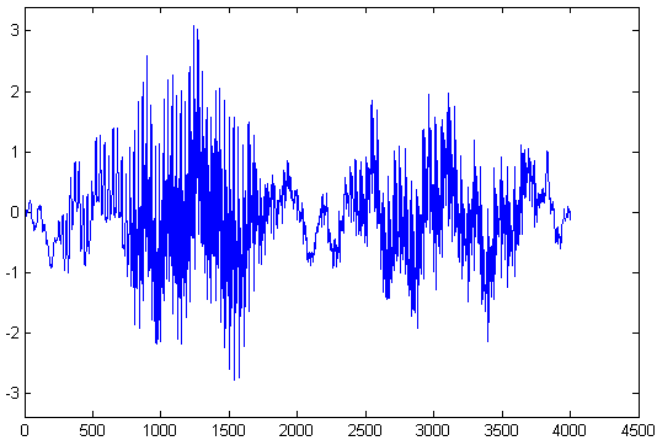

Fig. 10 Original Speech Signal

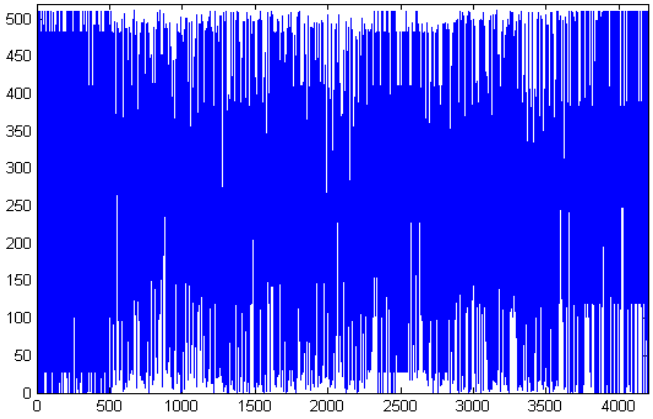

Fig. 11 Watermarked and Encrypted signal

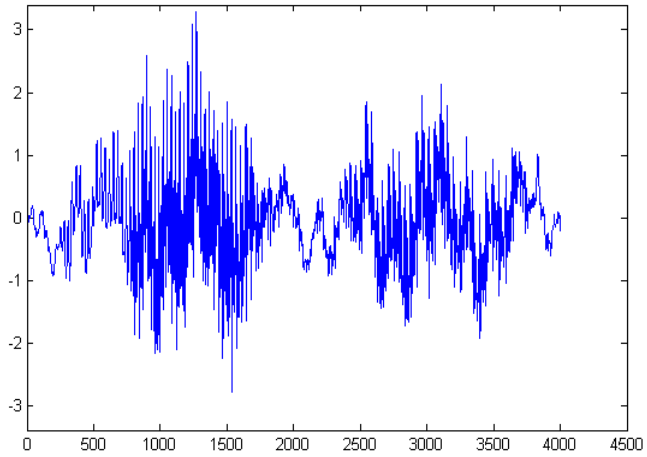

Fig. 12 Reconstructed signal at output

After decryption and elimination of watermark signal is reconstructed. Output signal is shown in Fig. 12. Output signal of Matlab is almost same to input signal, though non-linear down-sampling and reconstruction is performed.

Proposed scheme is implemented in Xilinx software, Signals from wave-editor of Xilinx software are shown in Fig. 13 - Fig. 16.

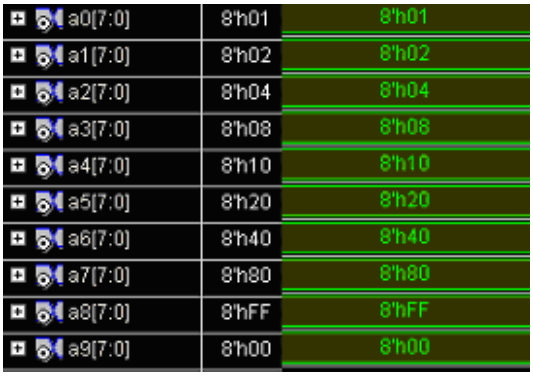

Fig. 13 Input frame, observed in waveform viewer of Xilinx software

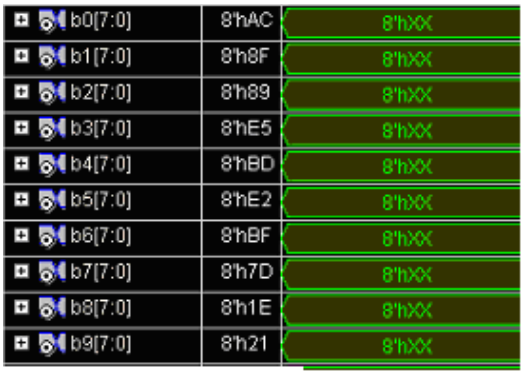

Fig. 14 Initial output, observed in waveform viewer of Xilinx software

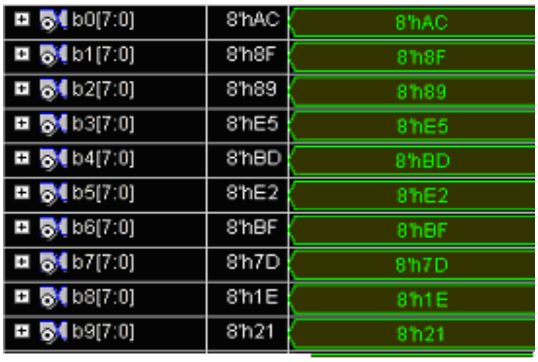

Fig. 15 Output after Encryption , observed in waveform viewer of Xilinx software

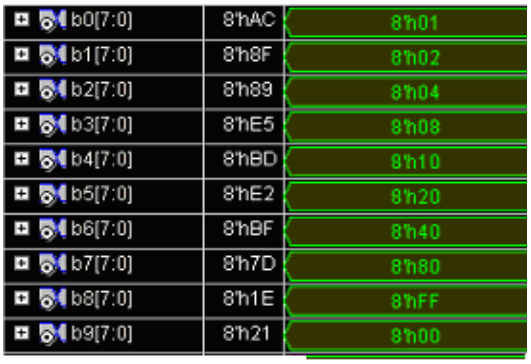

Fig. 16 Output after decryption, observed in waveform viewer of Xilinx software

After non-linear down-sampling compression 15-samples are compacted into 10-samples. Fig. 13 shows input samples (input frame), after compression. Output is don't care in Xilinx, (see Fig. 14) when clock of encryption is not triggered. Output of first FPGA is an encrypted frame. The encrypted frame is shown in Fig. 4. After decryption decrypted frame is found. Decrypted frame is same to original/input frame. Decrypted frame is shown at Fig. 15.

V DISCUSSION

In this paper, a secured realtime voice communication scheme is proposed and implemented it using FPGA and analyzed for several cases. Security analysis experimental results show that this cryptosystem will be a secured one. The proposed scheme has multi levels of security because encryption is performed using random number and the random bits are not easily guessable as they are not predictable. Compression makes space in the frame and facilitates the need of extra space for watermark and random numbers. Again watermark signal provides with necessary information and are hidden in the speech signal. They can be further used for authentication, user verification, copyright information and source tracing. The scheme saves the need for extra space. It is also good for high (Quality of Service) QoS [25] of data transmission as there is minimal latency from originating signal to the reconstructed signal. The proposed scheme is tested for speech signal with noise and found that it is suitable for a noisy environment.

Proposed scheme comprises of non-linear down-sampling compression, watermark and encryption portions. Compression creates vacancy for watermark and random signal. Watermark and random signal are inserted into the vacant locations. Finally encryption is performed. Brief discussion on proposed compression, watermark and decryption are discussed below.

A. Compression

Compression is taken to create space for watermark and random numbers. The non-linear down-sampling technique is used for compression. The technique is discussed in [22]. The main problem of this compression is sound quality loss for high-frequency speech signals. Loss-less compression techniques may also be used[23].

B. Watermark

Digital watermarking is the technique of inserting specific information into audio, data, image or video. The specific information is known as watermark and usually used for ownership verification, identification, authentication etc purposes and protection of integrity of data. Many watermarking schemes have been developed. These schemes can be classified as robust, fragile and semi-fragile approaches [10], [11]. Watermark information inserted repeatedly in each frame. So, the system is strong against watermark attacks. Such as copy-and-paste, counterfeiting and transplantation attacks.

C. Encryption and Decryption

The root of the word encryption—*crypt*—comes from the Greek word *kryptos*, meaning hidden or secret. Encryption is the method of hiding data form unwanted users.

In its earliest form, people have been attempting to conceal certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures. For different reason humans have been interested in protecting their messages. Early Chinese and Assyrians merchants encrypted their prices of goods [26-27].

Speech encryption was first proposed to satisfy the demand of military [28], and always plays an important role in military use. Crypto (cryptography) algorithms [29-33] are the core of such security systems, offering security services of data privacy, data integrity, authenticity and non-repudiation [34]. The Advanced Encryption Standard Algorithm [35-36] (AES) is used as the most trustworthy and commonly used algorithm for encrypting data. But AES is not a fast method in execution and frames are made interdependent for secured encryption. As frames are interdependent all frames will be garbage, if one frame is lost during trans-mission. In proposed technique random numbers are generated in each frame and other bits are encrypted using this random numbers. This ensures high security and doing so frames are not interdependent. So, it is an efficient technique for realtime implementation.

The proposed system also prevents all known attacks. Known attacks are Brute Force Attack, Parallel Attack, Cold Boot Attack, Malicious Code, Known Plaintext Attack, Man-in-the-Middle Attack and Differential Cryptanalysis.

Brute force attack is based on guessing the password or the encryption key. Key/password is determined by trial and error method. This method is performed using a number of computers in Parallel attack. Cold Boot Attack is for the systems, using RAM. In Man-in-the-Middle Attack (MIM, or MITM) attacker knows inputs and corresponding outputs of encryption system.

Proposed system prevents these attacks as it is a hardware-based encryption technique [37- 38], no external device (such as RAM) is used for encryption and output changes simulation to simulation for same input.

D. Transmission Technique

The proposed encryption-decryption system is not suitable for data facing bit error. Rather it is suitable for internet data transferring, where any lose of data is identified but not corrected. That means this method is useable for those data transmission where bit error does not occur (have very low probability of error) or bit error is identified by inspection,

such as check-sum method. In condition of any error one frame should be dropped.

It is also suitable for uploading and downloading voice-data. In realtime application frame should be dropped when an error occurs.

VI CONCLUSIONS

A new hardware-based secured audio communication scheme for realtime speech signal is presented in this publication which can be used for identification, ownership verification and authentication. The watermark is not easily detectable as the size of the frame is not increased and the watermark is buried in the signal. If there is any attempt to change the content of the signal in the transmission channel, proposed scheme can detect it and return noise at the end. The encryption is also completed with random block selection, random number and private key. So, if any other decryption algorithm is used, it also returns just noise at end. Thus it prevents network threats like eavesdropping, Man-in-the-Middle attack. It is only possible to extract original signal when proposed algorithm and key is known to person/ device, receiving the signal. Thus it can provide security for secure voice communication among the branches of an enterprise. Moreover, the user requires less buffer and memory space because of compression.

REFERENCES

[1] Z.M. Lu and S.H. Sun, "Digital Image Watermarking Technique Based on *Vector Quantization," Electronic Letters*, Vol. 36, No. 4, pp. 303-305, 2000.

[2] Valiulis, Carl. "Electronic identification, control, and security system and method for consumer electronics and the like." U.S. Patent No. 6,317,028. 13 Nov. 2001.

[3] Chien, Hung-Yu, Jinn-Ke Jan, and Yuh-Min Tseng. "An efficient and practical solution to remote authentication: smart card." *Computers & Security* 21.4 (2002): 372-375.

[4] Giorgio, Agostino. "A Wireless Electronic Device for the Personal Safety of Chronically Ill Persons for Indoor and Outdoor Use." *Consumer Electronics Times*.

[5] Pun, Chi-Man, Jing-Jing Jiang, and CL Philip Chen. "Adaptive Client-Side LUT-Based Digital Watermarking." *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*. IEEE, 2011.

[6] Grosges, Thomas, and Dominique Barchiesi. "Toward nanoworld-based secure encryption for enduring data storage." *Optics letters* 35.14 (2010): 2421-2423.

[7] Theocharis, Stamatios A., and George Tsihrintzis. "E-administration: Back-office systems upgrading the greek case." *Information Society (i-Society), 2012 International Conference on*. IEEE, 2012.

[8] Goyal, Vishal, U. S. Pandey, and Sanjay Batra. "Mobile Banking in India: Practices, Challenges and Security Issues." *International Journal* 1.2 (2012).

[9] Bilal, Muhammad. "Trust & Security issues in Mobile banking and its effect on Customers." (2011).

[10] C. I. Podilchuk, E. J. Delp, "Digital Watermarking: Algorithms and Applications," *IEEE Signal Process. Mag.,* Vol. 18, no 4, pp. 33-46, Jul. 2001.

[11] E. Izquierdo and V. Guerra, "An Ill-posed Operator for Secure Image Authentication," *IEEE Trans. Circuits Syst. Video Technol,* Vol. 13, No. 8, pp. 842852, Aug. 2003.

[12] L. Cai, R. Tu, J. Zhao, and Y. Mao, "Speech Quality Evaluation: A New Application of Digital Watermarking," *IEEE Transaction On Instrumentation And Measurement,* Vol. 56, No. 1, Page: 45-55 February 2007.

[13] P. Kitsos. N. Sklavos. and 0. Koufopavlou, "An Efficient Implementation of the Digital Signature Algorithm," *9th IEEE International Conference on Electronics: Circuits and Systems,* Pmc. of the. VoL3, San he. USA. 2002.

[14] S. 0. Med, A K Katsaggelos, and M. Sartafzadeh, "Analysis and FFGA Implementation of Image Restoration Under Resource Con-WainUC," *IEEE Trans. on Computers,* Vol 52. no.3, Mar. 2003.

[15] M. Klimerh, V Swton. and D. Walola, "Robust Image Watermarking Algorithm Based on Predictive Vector Quantization," *Proc. ICICIC06,* Vol. 3, pp. 491-494, 2006.

[16] Hordworr lmplemcwion of a Losskss Image Compnsrion Algorithm Using (I Field Pmgmrrnnble Gate Array, *TMO Rogrrss Repon,* pp. 42-144. Feb. 2001.

[17] Anoop MS, "Public Key Cryptography-Applications algorithm and mathematical explanations," 2007.

[18] Teerakanok, Thongpon; Kamolphiwong, Sinchai "Accelerating asymmetric-key cryptography using Parallelkey Cryptographic Algorithm (PCA)," *Telecommunications and Information Technology, 6th International Conference on computer,* Volume 02, pp.812 815, 2009.

[19] Advanced Encryption System, "Robust Image Watermarking Algorithm Based on Predictive Vector Quantization," *Federal Information Processing Standards Publication,* vol. 197, 2001.

[20] J. Daemen and V. R. Rijndael, "The advanced encryption standard," *Dr. Dobbs J.*, Vol. 26 No 3, pp.137139 , 2001.

[21] *National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standards Publication,* U.S. Government Printing Office, Washington, DC (1977).

[22] H. M. D. Kabir et al., "Non-linear Down-sampling and Signal Reconstruction, Without Folding," *in European Modelling Symposeum (EMS 2010),* 17-19 Nov. 2010.

[23] H. M. D. Kabir et al., "A Theory of Loss-less Compression of High Quality Speech Signals with Comparison," *in European Modelling Symposeum (EMS 2010),* 17-19 Nov. 2010.

[24] DeHon, André. "The density advantage of configurable computing." *Computer*33.4 (2000): 41-49.

[25] Tuoriniemi, A.; Eriksson, G.A.P.; Karlsson, N.; Mahkonen, A. "QoS concepts for ip-based wireless systems," *3G Mobile Communication Technologies*, pp. 229-233, 2002.

[26] F. Bacon, "De Augmentis Scientarum", *Bacon: Book 6, Chapter I.* [as quoted in C. Stopes, "Bacon-Shakspere Question", 1889.

[27] V. Senk, V. D. Delic, V. S. Milosevic, "A new speech scrambling concept based on Hadamard matrices", *IEEE Signal Processing Letters,* vol. 6, no. 4, pp. 161C-163, 1997.

[28] S B Alam, R Bulbul, H M D Kabir, "Real-time Speech Signals for E-Wallet using Watermarking Algorithm with Fast and

Highly Secured Encryption" in *International Journal of Mobile & Adhoc Network*. Vol. 1, Issue. 2, August 2011.

[29] S B Alam, R Bulbul, H M D Kabir, "Field Programming Oriented Secured Speech Communication using Watermark with Multiple Domain Analysis" in *International Journal of Mobile & Adhoc Network.* Vol. 1, Issue. 2, August 2011.

[30] [30] H M D Kabir et al., "Hardware based realtime, fast and highly secured speech communication using FPGA", in Proc. of *IEEE International Conference on Information Theory and Information Security (ICITIS)*, pp. 452-457. 17-19 Dec., China, 2010.

[31] Kabir , H M D et al., "Watermarking with fast and highly secured encryption for real-time speech signals", in Proc. of *IEEE International Conference on Information Theory and Information Security (ICITIS)*, pp. 446-451. 17-19 Dec., China, 2010.

[32] S B Alam, H M D Kabir, C Shahnaz, S A Fattah, "A Secured Electronic Transaction Scheme for Mobile Banking in Bangladesh Incorporating Digital Watermarking" in *International Conference on Information Theory and Information Security*, ICITIS 2010, Beijing, China, 17-19 Dec, 2010.

[33] S B Alam, A B M Rafi Sazzad, M N Sakib, H M D Kabir, C Shahnaz, S A Fattah, "Manipulation and Transparency Control of ICT constituted E-Administrative Protocol via Digital Watermarking for LDC's" in I*nternational Conference on Information Theory and Information Security, ICITIS 2010*, Beijing, China, 17-19 Dec, 2010.

[34] P. C. van Oorschot, A. J. Menezes, and S. A. Vanstone, *Handbook of Applied Cryptography,CRC press Inc.*, Florida, 1996.

[35] R. Ashruf, G. Gaydadjiev, S. Vassiliadis, "Reconfigurable Implemen-tation for the AES Algorithm", *Packet Switches, Journal of networks,* vol. 2, no. 3, pp. 28-35, June 2007.

[36] M. Mali, F. Novak, A. Biasizzo, "Hardware Implementation of AES Algorithm", *Journal of Elentrical Engineering,* VOL. 56, NO. 9-10, pp. 265-269, 2005.

[37] E. P. Guillen, D. A. Chacon, "VoIP Networks Performance Analysis with Encryption Systems", *World Academy of Science, Engineering and Technology*, 5 August 2009.

[38] Kabir, H M D, S B Alam. "Fast & Low-Power Consuming SRAM Design by Fast Precharging Using Equalizer and Sense Circuit." *Journal of Electron Devices* 9.20011: 325-334.

Hussain Mohammed Dipu Kabir received baccalaureate degree from Department of Electrical and Electronics Engineering of Bangladesh University of Engineering & Technology (BUET) in 2011.

Currently he is working at Advanced R&D Department of Samsung Bangladesh R&D Center. He also served as a reviewer in many IEEE conferences since the time his undergraduate study. Conferences are PECON, IAPEC, SCORED, ISIEA, ICEDSA, BEIAC, ICCSII etc.

His research interests are Efficient SRAM design, Audio codec development, Signal processing, Cryptography, Nuclear energy, Watermarking, VLSI design and Solid-state devices.

Saeed Anwar received baccalaureate degree from Department of Electrical and Electronics Engineering of Bangladesh University of Engineering & Technology (BUET) in 2011. Currently he is studying at University of Akron as a graduate student.

Abu Shahadat Md. Ibrahim completed his B. Sc. from Bangladesh University of Engineering and Technology (BUET) in Electrical and Electronic engineering with first class in 2008. He worked as Supply Chain Team Leader in British American Tobacco Bangladesh for four years. Currently he is a graduate student of University of Dhaka.

Dr. Mohd. Liakot Ali graduated from Bangladesh University of Engineering and Technology (BUET) in Electrical and Electronic engineering with first class in 1993. He obtained his MSc. from the National University of Malaysia (UKM) in Electrical, Electronic and Systems Engineering in 1998. He completed his PhD from Universiti Putra Malaysia (UPM) in Micro-electronic Engineering in 2004.

He started his career as a System Engineer in Advanced Computers & Information Technology, Dhaka, Bangladesh (Jan, 1994 - July, 1995). Then he joined as a Research Assistant in the National University of Malaysia (UKM) (July, 1995 - Nov, 1997), as an R & D Engineer in Leapfrog Technology Sdn. Bhd., Malaysia (Nov, 1997-Oct, 2000) and as a Senior Electronic Engineer in KUB Research Sdn. Bhd., Malaysia (Nov, 2000 - March, 2001). During his service in the company, he designed and developed few commercial advanced electronic products, which are being sold all over the world. Then He joined as a Lecturer in the Department of Electrical and Electronic Engineering, Universiti Putra Malaysia (UPM). He got excellent service certificate from the vice chancellor of the University. Currently, he is working as a Professor in the Institute of Information and Communication Technology, Bangladesh University of Engineering and Technology. Among the subjects he taught include Digital Circuits and Systems, Analog Circuits and Systems, Microelectronic Principles, VLSI Testing, Embedded System design etc. His current research interest includes: VLSI design and Testing, Micro-controller/Digital signal processor based advanced electronic product design.

Dr. MD. Abdul Matin received B,Sc degree from Bangladesh University of Engineering & Technology (BUET) in 1971. He received M. Sc. Engg from Tohoku University, Sendai, Japan in 1978. Area of Specialization of his M. Sc. was Electrical Communication Engineering. He received Ph. D from Tohoku University, Sendai, Japan in 1981. Area of Specialization of his Ph. D was Electrical Communication Engineering. He served as Assistant Professor in Department of Electrical and Electronic Engineering, BUET, Dhaka, Bangladesh from 13 May 1981 to 3 September 1984. He served as Associate Professor, Department of Electrical and Electronic Engineering, BUET, Dhaka, Bangladesh from 4 September 1984 to 1 January 1988.

He is serving as Professor Department of Electrical and Electronic Engineering, BUET, Dhaka since 2 January 1988. He was Head in Department of Electrical and Electronic Engineering, BUET, Dhaka from November 12, 1988 to November 11, 1990. As head of the Department, he procured huge quantity of laboratory equipments under Japanese International Cooperation Agency (JICA) Technical Assistance. He received the Best Supervisor Award on the Best Poster Paper of the EU Pro 09.

His research interests are Microwave Engineering, Antennas and Propagation, Applied Electro-Magnetics, Wireless and Mobile Communication Systems, Antennas in Plasma and Plasma Instability, WiMAX and GPS Systems, Nuclear Power Generation and Nuclear waste management.