Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 2; January-March, 2016, pp. 116-118

http://www.krishisanskriti.org/Publication.html

Speech Secret Sharing

Shivendra Shivani[1] and Suneeta Agarwal[2]

[1,2]National Institute of Technology, Allahabad
E-mail: [1]shivendrashivani@gmail.com, [2]suneeta@mnnit.ac.in

Abstract—*This paper proposes a novel Speech Secret Sharing approach using basics of visual cryptography. When a speech signal is transmitted over internet, it may be monitored and tampered intentionally or unintentionally. Hence confidentiality must be maintained during transmission. In proposed approach speech signal is secretly shared into two encrypted signals. No one can infer about original signal only by using one share. Experimental results show the effectiveness of the proposed approach.*

1. INTRODUCTION

Secret sharing is one of the important application of Visual Cryptography (VC). Secret may be image, speech or video. In this paper speech signal has been taken in our consideration. When speech signal [4][5] is broadcasted then it is very necessary to encode signal so that only an authority with valid license can only take enjoy of that speech signal. In this paper fundamental of visual cryptography is used to encode a speech signal.

VISUAL cryptography (VC) is a category of secret sharing scheme, proposed by Naor et al. [1], that allows the decoding of concealed images without any cryptographic computation. Mainly in a k-out-of-n visual secret sharing (VSS) scheme, a secret image is encoded into n shares. Each share resembles an unsystematic binary pattern. The shares are then printed onto transparencies, respectively, and distributed among n participants. Since isolated share has no visual information of the secret image but it can be visually exposed by just superimposing together any k or more transparencies of the shares without any cryptographic computation. In spite of having infinite computation power, k − 1 or fewer participants can not decode the secret image. Besides the secret sharing, visual cryptography can also be used for number of purposes including access control, watermarking, copyright protection [2], identification [3] and visual authentication. To demonstrate the principles of VSS, consider a trivial 2-outof-2 VSS (k = 2;n = 2) scheme shown in Fig. 1. Each pixel p of secret binary image is encoded into a pair of black and white subpixels for both shares. If p is white/black, one of the first/last two columns tabulated under the white/black pixel in Fig. 1 is selected randomly so that selection probability will be 50%. Then, the first two subpixels in that column are alloted to share 1 and the following other two subpixels are alloted to share 2. Independent of whether p is black or white, pixel is encoded into two subpixels of black-white or white-black with equal probabilities. Thus an

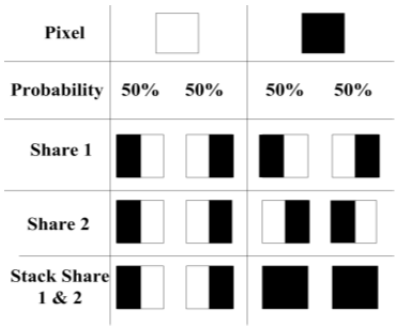

Fig. 1. 2-out of 2 VSS, where a secret pixel is encoded into two subpixels in each of the two shares

individual share has no idea about whether p is black or white. The last row of Fig. 1. shows the superimposition of the two shares, If the pixel p is black, the output of superimposition will be two black subpixel corresponding to a grey level 1. If p is white, Proposed then result of superimposition will be one white and one black subpixel, corresponding to a grey level 1/2. Hence by stacking two shares together, we can obtain the full visual information of the secret image.

2. SPEECH SECRET SHARING

Proposed approach consists of three algorithms as shown in Fig. 2. First of all recorded speech is converted into unsigned eight bit integer form so that each sample of signal can be further converted into eight bit binary form. This bit vector is denoted by S_b . To encrypt each bit we call Algorithm 2 (Secret Share Generation). This algorithm will call Algorithm 1 for basis matrix creation.

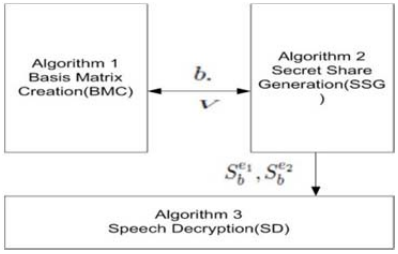

Fig. 2: Block diagram of proposed speech secret sharing approach.

Each binary bit will be encrypted by two bits 01 or 10 irrespective of 1 or 0. Hence it will be very difficult to identify the belonging secret bit only by seeing one share. At the receiver end, to decrypt the encoded speech, we require both shares. According to Algorithm 3, we just take logical OR operation on two consecutive bits. Finally if ORed bits are 01 or 10 then it will be treated as 0 otherwise 1.

Algorithm 1 Algorithm for Basis Matrix Creation(BMC)

INPUT: b.
OUTPUT: V.
Define: 1) b is single bit
2) V is matrix of dimension 2×2 where $V(1)$ and $V(2)$ indicate 1st and 2nd row of V

```
procedure BMC(b)
    if b = 0 then
        V(1) ← 01 or 10
        V(2) ← 01 or 10
    else
        V(1) ← 01 or 10
        V(2) ← 10 or 01
    end if
    Return b
end procedure
```

Algorithm 2 Algorithm for Secret Share Generation (SSG)

INPUT: S_b.
OUTPUT: $S_b^{e_1}, S_b^{e_2}$.
Define: 1) $\|$ shows the concatenation operation.
2) V is matrix of dimension 2×2 where $V(1)$ and $V(2)$ indicate 1st and 2nd row of V

```
procedure SSG(S_b)
    for i ← 1 to length(S_b) do
        V ← Call(BMC(S_b(i)))
        S_b^{e1} ← S_b^{e1} || V(1)
        S_b^{e2} ← S_b^{e2} || V(2)
    end for
    Return S_b^{e1}, S_b^{e2}
end procedure
```

Algorithm 3 Algorithm for Speech Decryption(SD)

INPUT: $S_b^{e_1}, S_b^{e_2}$.
OUTPUT: S_r.
Define: 1) S_r is a empty vector of length same as S_b

```
procedure SD(S_b)
    while i ≠ length(S_b^{e1}) do
        B ← OR(S_b^{e1}(i, i+1), S_b^{e2}(i, i+1))
        if B = 01 then
            S_r ← S_r || 0
        else
            S_r ← S_r || 1
        end if
        i ← i + 1
    end while
    Return S_r
end procedure
```

3. EXPERIMENTAL RESULTS

Experiments have been performed on various speech signals. Though the encrypted signals in the form of shares are twice in length but it assures security and recovery of original signal 100 %. Fig. 3 is the demonstration of one of the speech signal and its shares. One can see that the similarity between Fig 3 (a) and (d). It shows that we can recover speech signal with 100% accuracy. Similarity is also measured with various objective and subjective evaluation parameters.

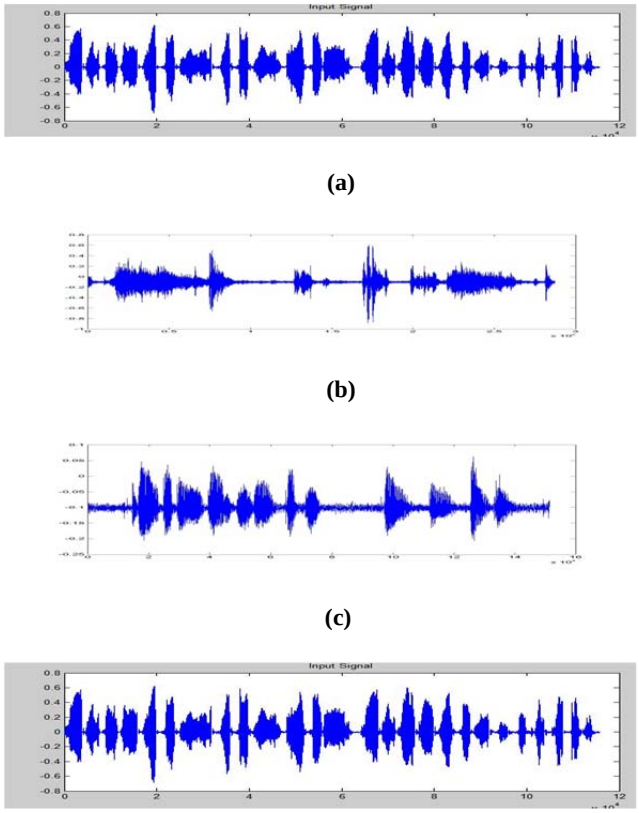

Fig. 3: Experimental result where (a) Input signal which is going to be encrypted (b) and (c) are two secret shares. (d) Decrypted signal.

4. CONCLUSIONS

In this paper, we have proposed a novel Speech Secret Sharing approach using basic principles of visual cryptography. Secret sharing is one of the vital application area of visual cryptography. Secret may be image, speech, video or text. In proposed approach, we have focused on secretly sharing the speech signals. It is very useful application for broadcast monitoring and securing a signals by unauthorized intruders. Here speech signal is secretly shared into two encrypted signals. No one can infer about original signal only by using

one share. Experimental results show the effectiveness of the proposed approach.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT94, LNCS, vol. 950, pp. 112, 1995.

[2] M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking," in Proc. IEEE Int. Conf. Multimedia and Expo, Taipei, Taiwan, Jun. 2004.

[3] M. Naor and B. Pinkas, "Visual authentication and identification," Crypto97, LNCS, vol. 1294, pp. 322340, 1997.

[4] Rabiner, Lawrence R., and Ronald W. Schafer. *Digital processing of speech signals*. Prentice Hall, 1978.

[5] Parsons, Thomas W. *Voice and speech processing*. McGraw-Hill College, 1987.