Design and Implementation of Multilevel Access Control in Medical Image Transmission Using Symmetric Polynomial Based Audio Steganography

J. Nafeesa Begum
Research Scholar & Sr. Lecturer in CSE, Government College of Engg, Bargur-635104, Tamil Nadu, India
nafeesa_jeddy@yahoo.com

K. Kumar
Research Scholar & Lecturer in CSE, Government College of Engg, Bargur-635104, Tamil Nadu, India
pkk_kumar@yahoo.com

Dr. V. Sumathy
Asst. Professor in ECE, Government College of Technology, Coimbatore, Tamil Nadu, India
sumi_gct2001@yahoo.co.in

Abstract— Steganography techniques are used in Multimedia data transfer to prevent adversaries from eavesdropping. The medical profession is also under a strict duty to protect the confidentiality of patients’ medical records as per the HIPAA ACT of 1996. Thus, protection of medical data/information in telemedicine is of paramount importance. Most telemedicine include some form of security measures such as the use of passwords. Password identification determines whether a user is authorized to gain access to a system. However, passwords are insufficient mechanisms to maintain patient confidentiality from intruders who gain knowledge of a user's password to log onto a system. This paper deals with the design and implementation of multilevel access control in medical image transmission using symmetric polynomial based audio steganography. Medical image transmission using audio steganography deals with covering the medical image on top of an audio file and subsequently sending it to multiple receivers. Only the intended recipients know that the audio file actually contains medical images and they can use their key to see the images. We have developed a Multilevel access control model by which medical images sent to low class users like medical assistants can also be seen by physicians who are higher in the hierarchy whereas the vice-versa is not allowed. To provide multilevel access control, symmetric polynomial based scheme is used. The steganography scheme makes it possible to hide the medical image in different bit locations of host media without inviting suspicion. The Secret file is embedded in a cover media with a key. At the receiving end the key can be derived by all the classes which are higher in the hierarchy using symmetric polynomial and the medical image file can be retrieved. The system is implemented and found to be secure, fast and scalable. Simulation results show that the system is dynamic in nature and allows any type of hierarchy. The proposed approach performs better even during frequent member joins and leaves. The computation cost is reduced as the same algorithm is used for key computation and descendant key derivation. Steganographic technique used in this paper does not use the conventional LSB’s and uses two bit positions and the hidden data occurs only from a frame which is dictated by the key that is used. Hence the quality of stego data is improved.

Index Terms— HIPAA, Steganography, Multilevel Access control, audio file, symmetric polynomial, dynamic, scalable

INTRODUCTION

The Health Insurance Portability and Accountability act (HIPAA) is widely acknowledged as the norm for healthcare services and Indian companies are well versed with the Act and other regulatory bodies. HIPAA [25] covers all protected healthcare information. It does not apply to specific records, but to information. The information is protected in any form by HIPAA and it continues to apply whether the content is being printed, discussed orally, or changes in form. For organizations that deal with the electronic management of healthcare information it is vital to protect the electronic maintenance and transmission of this data. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size.

There are many scenarios in which situation arises that only some users should be able to view the medical image or all higher level users should also be able to view the image message that is relayed to the doctors. For example in a orthopedic hospital all messages sent to surgeons should be seen by the pathologists, radiologists, anesthetologists who are actually invisible doctors but play an important role in the operation by guiding the surgeon. There may be many other images sent to pathologists, radiologists, anesthetologists that
need not be known to the surgeons. Like wise all images sent to medical students need to be sent to the chief physician. There should also be a mechanism by which people at the same level are able to converse among themselves.

To implement such a multilevel access control in steganography symmetric polynomial approach is used. In most existing schemes, key derivation is different from key computation. Key derivation needs iterative computation of keys for nodes along the path from a node to its descendant, which is inefficient if the path is long. In this scheme, both operations are same by substituting (different) parameters in the same polynomial function assigned to node v. Thus, the key derivation efficiency can be improved. Our scheme also supports full dynamics at both node and user levels and permits any random access hierarchies. More importantly, removing nodes and/or users is an operation as simple as adding nodes and/or users in the hierarchy. A trusted Central Authority (CA) can assign secrets (i.e. polynomials) to corresponding nodes so that nodes can compute their keys. Also, nodes can derive their descendant’s keys without involvement of the CA once polynomial functions were distributed to them. In addition, the storage requirement and computation complexity at the CA are almost same as that at individual nodes, thus, the CA would not be a performance bottleneck and can deal with dynamic operations efficiently.

The rest of the paper is as follows, Section 2 deals with related work Section 3 gives all overview of the system Section 4 describes the audio steganographic method for the images Section 5 deals about the symmetric polynomial approach Section 6 shows the simulation results and Section 7 gives the performance analysis and section 8 concludes the paper.

II. RELATED WORK

Information hiding using steganography [9] relates to protection of text, image, audio and digital content on a cover medium [1,2,3,5]. The cover media in many cases has been an image [1]. Aoki presented a method in which information that is useful for widening the base band is hidden into the speech data [6]. Sub band Phase shifting was also proposed for acoustic data hiding [3]. All these schemes focus on data that is stored in a hard disk or any other hardware whereas there are many applications like military warfare where the audio data is to be given in real time as in live broadcast system. Techniques for hiding the audio in real time came into existence [4] and systems for synchronized audio steganography has been developed and evaluated [7]. In this scheme secret speech data is recorded and at the same time it is sent to the receiver and a trusted receiver extracts the speech from the stego data using the key which is shared between the server and the receiver. In the proposed scheme multilevel access control is implemented using symmetric polynomial approach. The audio is encrypted by a key of lower level user, and the higher level users are able to derive the key using symmetric polynomial approach. Forward and Backward secrecy [8] i.e. whoever is active at that instance only are able to receive the audio.

The first multi level access solution was proposed by Akl et al. [11, 12] in 1983 and followed by many others [13, 16, 17, 18, 20, 21, 14, 15, 19, 22, 23]. These schemes basically rely on a one-way function so that a node v can easily compute v’s descendant’s keys whereas v’s key is computationally difficult to be computed by v’s descendant nodes. Moreover, many existing schemes have some of the following problems: (1) Some schemes were found with security flaws in due course of time shortly after they were proposed; (2) Some schemes cannot support for reconfiguration of a hierarchy; (3) Some schemes require access hierarchy to be in a certain form so that it must be a tree or a DAG with only one root; and (4) Member revocation is one of the most difficult processes in cryptographic schemes, therefore, it is important to address this problem so that the revocation process can be dealt with efficiently. In this paper, we propose a new scheme based on symmetric polynomials for synchronized audio data. Unlike many existing schemes based on one-way functions, our scheme is based on a secret sharing method which makes the scheme unconditionally secure [21, 24]. Also, this multilevel access control requires two types of key operations: (1) key computation: a node v computes its own key, and (2) key derivation: a node v computes its descendant’s keys.

III. SYSTEM OVERVIEW

Multilevel Access Control in medical image transmission is useful for Hospitals which have a hierarchical structure. For e.g. In a Orthopedic hospital, many people are involved at various levels and there is a hierarchy among them as shown below.

Figure: 1 : A sample hierarchy in a medical organization
In such a type of system, medical images sent to a lower class should be seen by the active members of lower class and also by all active members of the higher class. It is not only essential to maintain the access control but, the data should be hidden as well. Steganography technique is used to hide the image into audio file and sent. The sequence of events is as follows.

**At the server**
1. Generate a general polynomial.
2. Give a symmetric polynomial to each of the classes.
3. Select the image to be sent
4. Use Steganographic technique to hide the image into audio.
5. A text can also be hidden in a audio file.
6. The file is encrypted by the class key for whom the message is to be relayed.
7. The symmetric polynomial generates a key in this case.
8. The server takes care of including class dynamics so the hierarchy can be changed at any time.
9. Users can join or leave a class at all instances. Keys are recalculated so that Forward and Backward secrecy are maintained.
10. If the users within the group need to transfer message among themselves, the private key of the users is used.

**At the receiver**
1. All the active receivers will receive the audio file.
2. If the recipient belongs to the actual intended class he can use the polynomial to get the hidden medical image file instantaneously from the audio file.
3. If the recipient belongs to a class lower than the actual intended class in the hierarchy, he will not be able to derive the key. The polynomial derivation method will give a null value.
4. If the recipient belongs to a higher class he can derive the key of the lower class and see the image file which in turn is applicable to text messages as well.
5. The users at the same class can transfer messages among them.
6. When a user joins or leaves, the new polynomials are given by the server and the private keys also get updated according to the new polynomial. Other classes are not affected by this.
7. Service messages can be sent from higher class users to lower class users.
3.1. Contribution
Solutions of a synchronized steganography have been given in past [7]. In this once the stego data reaches the destination the audio can be listened by the trusted receiver. Our contributions are
1. The key is used during the embedding process also.
2. The key is not a simple key but it identifies a class of users.
3. If the key used belongs to a low level group in the hierarchy, the higher level class of user can derive the key using the symmetric polynomial approach and listen to it.
4. There can be normal message transfer among the group elements and also service messages from higher classes.
5. Forward and backward secrecy is maintained.
6. It is a dynamic one where new hierarchies can be introduced, User level and class level dynamics are taken care.

IV AUDIO STEGANOGRAPHY FOR MEDICAL IMAGES
The input Image to be sent is selected. When the covering media is being played at the same time the image is can be put into the audio file simultaneously or the image can as well be hidden in a already stored file. The stego bit stream is then transmitted to the receivers. Multilevel Access control using symmetric polynomial is used at this stage to generate the key to make secure transmission of the image file. According to the hierarchy the trusted users are able to retrieve the hidden audio file.

In this system, cover data is divided into fix-sized frames according to Pulse Code Modulation setting. To cover low size and high phonetic quality suitable sampling rate for the cover media is selected. Three main processes are involved in the Audio Steganography for Medical Images.

1. Using data sampling image data’s are embedded into another audio.
2. Bit Embedding: The key used helps in hiding the image file in bit positions and once the bit positions are found data is hidden after performing an operation on secret data along with the key.
3. Synchronized Process: Malicious and intentional attacks can be avoided as the secret data can be put over a real time audio input also.

4.1 Algorithm
Step1: select the image file. The audio file is divided into fix-sized frames according to Pulse Code Modulation setting. To cover low size and high phonetic quality suitable sampling rate for the cover media is selected. Three main processes are involved in the Audio Steganography for Medical Images.

1. Using data sampling image data’s are embedded into another audio.
2. Bit Embedding: The key used helps in hiding the image file in bit positions and once the bit positions are found data is hidden after performing an operation on secret data and the key.
3. Synchronized Process: Malicious and intentional attacks can be avoided as the secret data can be put over a real time audio input also.

4.1 Algorithm
Step1: select the image file. The audio file is divided into fix-sized frames and set to be specific PCM format. PCM qualification is decided by sampling rate, sampling size, and sampling channel. The PCM property of cover audio wav is set to be 32 kHz-16bit-2ch.

FORMULA USED FOR STEGANOGRAPHY:
Steganographic process:
cover medium + hidden data + stego_key = stego_medium

The format is being specified by a WAVEFORMATEX structure:

```
| 01 00 | 02 00 | 03 00 |
|-------|-------|-------|
| WAV_FORMAT_PCM | count of channels | samples per second |
| 44 0C 00 00 | 04 00 | 10 00 |
| bytes per second | block align | bits per sample |
```

Step2: Use Symmetric Polynomial to calculate key of class
Step3: Perform calculation and decide the frame from which the data is to be embedded.
Step4: Decide two bit locations in each frame and clear the bit in the locations .cmask1 = (2loc1−1) xor (Keybit), cmask2 = (2loc2−1) xor (Keybit), cmask = cmask1 ∧ cmask2 hide the secret data bits into these bit locations by again performing an operation on the secret data along with the key.
Step5: The next set of data will go to the next frame.
Step6: Do the repetitive process till the entire image is hidden.
Step8: Transmit using sockets
Step9: At the receiving end, Use the key and see the image
Step10: If the receiving user belongs to higher class, he can derive the key and listen to the audio.

V SYMMETRIC POLYNOMIAL APPROACH PROTOCOL
A polynomial F(x; y; z) is said to be symmetric if F(x; y; z) = F(x; z; y) = F(y; x; z) = F(y; z; x) = F(z; x; y) = F(z; y; x): A polynomial in several variables x1,..., xn is called symmetric if it does not change when you permute the variables.

5.1 A Symmetric Polynomial Based Multilevel Access Scheme
- A is an set of n classes – { C1,C2,C3,….,Cn}
- B is a set of ancestral classes of set A.
  B = {S1,S2,S2,…….,Sn}
- mi is calculated as the number of the ancestral classes
  mi = |Si|
- We are choosing a value for m, such that m ≥ max {m1,m2,m3,…….,mn} + 1
- Here m is the number of parameter in the polynomial function P, where P is for constructing our multi level access control scheme

A Numerical Example:

```
Figure 4: Hierarchical Structure of Multi Level access control
```

A Numerical Example:
Here we have nine classes
\{ C1,C2,C3,C4,C5,C6,C7,C8,C9 \}

Ancestral classes sets are

\[ S1 = \{ \varphi \} \]
\[ S2 = \{ \varphi \} \]
\[ S3 = \{ C1,C2 \} \]
\[ S4 = \{ C2 \} \]
\[ S5 = \{ C2 \} \]
\[ S6 = \{ C1,C2,C3 \} \]
\[ S7 = \{ C1,C2,C3,C4 \} \]
\[ S8 = \{ C2,C3,C5 \} \]
\[ S9 = \{ C2,C5 \} \]

From the previous step, we need to choose \( m \) such that
\[ m \geq \max \{ m1,m2,m3,\ldots.,m9 \} + 1 \]

Let us choose \( m=7 \), It will allow us to expand the hierarchy without changing the value of \( m \).

Symmetric polynomial, we are using here is as follows
\[ P(x1,x2,\ldots.,xm) = \sum_{i1=0}^{t} \sum_{i2=0}^{t} \ldots \sum_{im=0}^{t} a_{i1,i2,\ldots.,im} x_{i1}^{i1} x_{i2}^{i2} \ldots x_{im}^{im} \mod p \]

Here \( t \) is threshold number.

We can classify the work into two types.

i) Key Calculation

ii) Key Derivation

**Key Calculation**

We can calculate key \( K_i \) of class \( C_i \) as follows
\[ K_i = P(S_i,S_{i1},S_{i2},\ldots.,S_{im},S'_{i1},S'_{i2},\ldots.,S'_{m-mi}) \]  \( - (1) \)

**Key Derivation**

In key derivation, we are using a term \( S_j/I \) which can be calculated as
\[ S_j/I = S_j/(S_i \cup \{ Ci \}) \]
\[ = \{ C_{(j|i1)}, C_{(j|i2)},\ldots., C_{(j|i)} \} \]

Consider a class \( Ci \) which is ancestor to class \( Cj \) and key \( Kj \) can be calculated by \( Ci \) as,
\[ \begin{align*}
K_i &= g(S_j, S_{(j)i1}, S_{(j)i2},\ldots., S_{(j)i}), \\
    & \quad S'_{i1},S'_{i2},\ldots.,S'_{m-mi} \\
    & \quad S_{(j)i2},\ldots., S_{(j)i}, S'_{i1},S'_{i2},\ldots.,S'_{m-mi-2} \\
    & = P(S_{i1},S_{i2},\ldots.,S_{im},S_{(j)i1}, \\
    & \quad S_{(j)i2},\ldots., S_{(j)i}, S'_{i1},S'_{i2},\ldots.,S'_{m-mi-2}) \quad (2)
\end{align*} \]

**Example**

**Key Derivation**

Consider that \( C3 \) is an ancestor class to class \( C7 \). Then \( K7 \) can be derived by \( C3 \) in the following steps.
\[ S_{j3} = \{ C4 \} \]
\[ K7 = P(S3,S7,S1,S2,S4,S1',S2') \]

**Key Derivation of class 7 by class 3 using equation(2)**
\[ S3 = \{ C1,C2 \} \]
\[ S7 = \{ C1,C2,C3,C4 \} \]
\[ S7U\{ C7 \} = \{ C1,C2,C3,C4,C7 \} \]
\[ S7/3 = \{ \varphi \} \]
\[ K7 = P(S7,S1,S2,S3,S4,S1',S2') \]  \( - (3) \)

It can be seen that when the class derives its own key and when an ancestor of this class derives the key , equation 2 and equation 4 have same parameters passed in the polynomial but the combination differs whereas when a wrong ancestor derives the key the parameters are not the same.

The default values, we have taken are

1) \( m=7 \)
2) \( P=2147483646 \)
3) \( s1=5, s2=10,s3=13,s4=9,s5=6,s6=22,s7=18,s8=30, s9=39, \)

**General Concept used in the polynomial:**
\[ \text{for(i=0;i<t;i++)} \]
\[ \text{for(j=0;j<t;j++)} \]
\[ \text{for(k=0;k<t;k++)} \]
\[ \text{for(l=0;l<t;l++)} \]
\[ \text{for(m=0;m<t;m++)} \]
\[ \text{for(n=0;n<t;n++)} \]
\[ \text{for(o=0;o<t;o++)} \]
\[ \{ a[o] = o^2 + 10 \text{ } a[o] = a[o] \cdot a \cdot b \cdot c \cdot d \cdot e \cdot f \cdot g \} \]
\[ c = (c+a[o]) \mod s \]

**Key Calculation for the Classes using equation (1)**
\[ K1 = P(S1,S1',S2',S3',S4',S5',S6') \]
\[ K2 = P(S2,S1',S2',S3',S4',S5',S6') \]
\[ K3 = P(S1,S2,S3, S1',S2',S3',S4') \]
\[ K4 = P(S4,S1,S2,S1',S2',S3',S4') \]
\[ K5 = P(S5,S1,S2,S1',S2',S3',S4') \]
\[ K6 = P(S6,S1,S2,S3,r1,r2,r3) \]
\[ K7 = P(S7,S1,S2,S3,S4,S1',S2') \]  \( - (3) \)
\[ K8 = P(S8, S1,S2,S3,S4,S5,r1) \]
\[ K9 = P(S9, S1,S2,S3,S4,S5,r1) \]

**Key Derivation of class 7 by class 3 using equation(2)**
\[ S3 = \{ C1,C2 \} \]
\[ S7 = \{ C1,C2,C3,C4 \} \]
\[ S7U\{ C7 \} = \{ C1,C2,C3,C4,C7 \} \]
\[ S7/3 = \{ C4 \} \]
\[ K7 = P(S3,S7,S1,S2,S4,S1',S2') \]  \( - (4) \)

Which is equal to the key calculated by class 7 itself.

**Key Derivation of class 3 by class 7 using equation(2)**
\[ S3 = \{ C1,C2 \} \]
\[ S7 = \{ C1,C2,C3,C4 \} \]
\[ S7U\{ C7 \} = \{ C1,C2,C3,C4,C7 \} \]
\[ S7/3 = \{ \varphi \} \]
\[ K7 = P(S7,S3,S1,S2,S3,S4,S1',S2') \]  \( - (5) \)
For a small Hierarchy, with more than two classes, we can easily illustrate our key calculations, where each class consists of several users.

**Illustrations shown for the hierarchy below**

```
CLASS 1  USER11
         |
         |
CLASS 3  USER12
         |
         |
CLASS 2  USER13
         |
         |
CLASS 3  USER14
         |
         |
CLASS 4  USER15
         |
         |
CLASS 5
```

**Key Calculations:**

**Step-1:**

The parameters to be passed for calculating group key class 2 are

\[
P(s_2, r_1, r_2, r_3, r_4, r_5, r_6)
\]

Group key class C2

\[699615258\]

1) Private key for user41

\[1947982264+(1947982264/41)\]

\[=1995494026\]

2) Private key for user42

\[1947982264+(1947982264/42)\]

\[=1994362794\]

3) Private key for user43

\[1947982264+(194782264/43)\]

\[=1993284177\]

4) Private key for user44

\[1947982264+(194782264/44)\]

\[=1992254588\]

**Step-2:**

The same way group key for class 4 can also calculated by passing the following parameters to the polynomial

\[
P(s_4, s_2, r_1, r_2, r_3, r_4, r_5)
\]

Group key for class C4 = 1947982264

Private Keys are used for local communication among the users.

**VI. SIMULATION RESULTS**

The system is developed using .NET and found to be secure and fast. The system takes care of User level and Class level dynamics. The large number of numbers prevents a possible guessing. For a eight parameter polynomial, 16! (i.e. 10922789888000) combinations possible. Bursty leave and join operations also are possible and the system can be used for any hierarchy.

The additional features that are included are

1. message passing among the same group.
2. service messages from higher users to lower level users.
3. Dynamics at user level and class level and secrecy.
VII PERFORMANCE ANALYSIS:

Performance and security: Each user \( u_i \) will receive the time complexity for computing the group key is \( O(w^{2n}) \). An important performance measure for a secure group communication scheme is the number of rekeying messages. Suppose that \( t \) users will be joining the group. The TA will send \( k \) and \( g_i \) to each of them respectively (2t messages) and broadcast one message to tell which users are joining. The total number of rekeying messages is \( O(2t) \). Suppose that \( t \) users are leaving the group. The TA only broadcasts one message to tell which users are leaving, thus the number of rekeying messages is \( O(1) \). Suppose that \( t \) users are joining and another \( v \) user are leaving the group, the total number of rekeying messages is still \( O(2t) \). As for the security of the scheme, if \( w + 1 \) users collude, then they can figure out the function \( f \) entirely. Therefore, the scheme is \( w \)-resilient. Moreover, if less than \( w + 1 \) users collude, they cannot get any information about the key, i.e., any value in the key space looks like a valid and equiprobable key to these colluding users. It follows that

\[ g_i = f(x_1, x_2, \ldots, x_n) = g(x_2, \ldots, x_n) = \sum_{i=0}^{w} \sum_{j=0}^{w} a_{ij} x_1^i x_2^j \]

the scheme is unconditionally secure.

A. Memory: Each user will be able to calculate the key based on the polynomial and hence very less memory is used. All parameters are publicly available and using the same method keys of lower hierarchy can be derived by substituting the corresponding parameters as given by the derivation module. The steganographic module does not involve any storage for storing the already recorded data as always data is recorded and subsequently sent to the receivers. The size of the cover medium does not increase because only two bits are used in each channel.

B. Computation cost: When the user joins there is no need for recalculation because the recorded message has already been played. When a user leaves a group key is recalculated and given to the class. Private keys are generated from this. The value of the new key involves not a change of parameters but a change of mod P value. Hence each class will be able to get a new polynomial value by passing the same parameters. Any left user will not be able to get the key. Only one key is used during creation of stego data. The higher class users need not remember the keys of all their descendant classes but rather using a simple scheme derive the exact parameters to generate the key. Hence the computation cost is reduced.

C. Communication cost: The p value is changed by the Trusted Authority and when the users try to calculate the key the new key will be generated. The computation cost is reduced because, the class users are not bothered about the key transmission. Once the polynomial is given the users can calculate their own key.

D. Dynamics: Class joining, Class leaving, Dynamic Hierarchy and New user joining a class are all done by the trusted authority in a phased manner thereby allowing the scheme to scale to greater hierarchy. Additionally local messaging and service messages are taken care in this system.

VIII. CONCLUSION AND FUTURE WORK

Thus in this paper, Design And Implementation of Multilevel Access Control in Medical Image Transmission Using Symmetric Polynomial Based Audio Steganography is done. The implementation results show that any type of hierarchy can be introduced and all dynamics can be done. For a 8 parameter polynomial that can have 8 among the 16 values, there are 16! combinations. Also, nodes can derive their descendants’ keys without involvement of the CA once polynomial functions are distributed to them. In addition, the storage requirement and computation complexity at the CA are almost same as that at individual nodes, thus, the CA would not be a performance bottleneck and can deal with dynamic operations efficiently.
We believe that this flexible, integrated and easy to use solution is a robust alternative to more complex architectures for simple image transmissions or occasional circumstances. In many fields (e.g., medicine, manufacturing, veterinary science, scientific research, etc.), it is often necessary to examine a subject and communicate the results of the examination to a remote place. Such information exchanges are especially desirable in the medical arena where it is often useful for medical practitioners to communicate medical information, such as patient test results, e.g., radiology studies or cardiac studies, to other practitioners located in remote places. This type of system provides secure transmission with multilevel access control.

8.1 Future work
1. The Trusted authority can still make it secure by changing the value of the parameters.
2. Should be extended for video files.
3. Bit selection for steganography can be made by using some pseudo random generator.

REFERENCES
[1] Neil F. Johnson, Z.Duric and S.Jajodia. “Information Hiding Steganography and Watermarking—Attacks and Countermeasures”, Kluwer Academic Publishers, 2001.
[2] F.A.P. Petitcolas, R.J.Anderson, M.G.Kuhn:"Information Hiding - A Survey", Process of IEEE, vol.87, no.7, pp.1062-1078, July, 1999.
[3] Matsuoka Hosei. “Acoustic Data Hiding Method using Sub-band Phase Shifting”, Technical report of IEICE, EA vol.106 pp.7-11, 2006.
[4] Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. “The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream”, Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.
[5] Min Wu, Bede Liu. “Multimedia Data Hiding”, Springer-Verlag New York, 2003.
[6] Aoki Naofumi. "A Band Widening Technique for VoIP Speech Using Steganography Technology", Report of IEICE, SP,106(333), pp.31-36, 2006.
[7] Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe “Design and implementation of synchronized audio-to-audio steganography scheme”, pg331-334, IEEE explore 2008.
[8] G. Tsudik Y. Kim, A. Perrig, "Simple and fault-tolerant key agreement for dynamic collaborative groups," in Proceedings of the 7th ACM conference on Computer and communications security, November 2000.
[9] W. Stallings, editor. Network and Internetworking Security. Pearson Education Asia, 2001.
[10] Xukai Zou, Li Bai,"A new class of key management scheme for access control in dynamic hierarchies", CCR-0311577, 2000.
[11] S. G. Akl and P. D. Taylor. Cryptographic solution to a problem of access control in a hierarchy. ACM Transactions on Computer Systems, 1(3):239-247, March 1983.
[12] S. J. MacKinnon, P. D. Taylor, H. Meijer, and S. G. Akl. An optimal algorithm for assigning cryptographic keys to control access in a hierarchy. IEEE Transactions on Computers, 34(9):797.802, Sept. 1985.
[13] S. Chen, Y.-F. Chung, and C.-S. Tian. A novel key management scheme for dynamic access control in a user hierarchy. In COMPSAC, pages 396-397, Sept. 2004.
[14] I. Ray, I. Ray, and N. Narasimhamurthi. "A cryptographic solution to implement access control in a hierarchy and more", SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies, pages 65.73. ACM Press, 2002.
[15] R. S. Sandhu. Cryptographic implementation of a tree hierarchy for access control. Information Processing, Letter, 27(2):95.98, Feb. 1988.
[16] G. C. Chick and S. E. Tavares. Flexible access control with master keys. Proceedings on Advances in Cryptology: CRYPTO '89, LNCS, 435:316.322, 1989.
[17] M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phatak. Hierarchical key management scheme using polynomial interpolation. SIGOPS Operating Systems Review, 39(1):40.47, Jan. 2005.
[18] L. Harn and H. Y. Lin. A cryptographic key generation scheme for multilevel data security. Computers and Security, 9(6):539.546, Oct. 1990.
[19] V. R. L. Shen and T.-S. Chen. A novel key management scheme based on discrete logarithms and polynomial interpolations. Computers and Security, 21(2):164.171, Mar. 2002.
[20] M.-S. Hwang, C.-H. Liu, and J.-W. Lo. An efficient key assignment for access control in large partially ordered hierarchy. Journal of Systems and Software, Feb. 2004.
[21] C. H. Lin. Dynamic key management scheme for access control in a hierarchy. Computer Communications, 20(15):1381.1385, Dec. 1997.
[22] S. Zhong. A practical key management scheme for access control in a user hierarchy. Computers and Security, 21(8):750.759, Nov. 2002.
[23] X. Zou, B. Ramamurthy, and S. Magliveras. Chinese remainder theorem based hierarchical access control for secure group communications. Lecture Notes in Computer Science (LNCS), 2229:381.385, Nov. 2001.
[24] X. Zou, B. Ramamurthy, and S. S. Magliveras, editors. Secure Group Communications over Data Networks. Springer, New York, NY, USA, ISBN: 0-387-22970-1, Oct. 2004.
[25] www.hipaa.org.