SECURE STEGANOGRAPHIC AUDIO MESSAGE SENDING USING BLOWFISH AND SHA SECURITY

Monika Modi[1], Mr. Amarjeet Jhajharia[2]
[1]M.Tech. Scholar, [2]Asst. Professor, Department of Computer Science, Jagannath University,Jaipur, India.

Abstract: Data Transfer is the basis of any of the communication process. And the possibility is always there that the data can be captured by the intruders. In the processed work, we are dealing with the audo message transfer in this to securely transfer the text message we have embedded or hide the text message within the audio message using the key and the key will be required to extract the required message. To further enhance the security paradigm, we have added up the concept of validating the user and encrypting the image of the users using the blowfish and latter in the process of transferring the message, first finger print and transaction id are validated then the message is send.

Keyword: Encryption, Decryption ,Stegnography

I. INTRODUCTION

Security has dependably been a vital part of human. We are encompassed by a universe of secure communication, where individuals of different types are transmitting data such as credit card number to an online store than and as cunning as a terrorist plot to hijackers. The strategies that make secure communication practicable are not new. There has dependably been a need of securing the messages that are sensitive in nature. Such messages if presented to a few intruders may represent a risk to country's security or organization's basic choices. Therefore, such data must be secured at any expense and to fill the need to encrypt or hide the data. Cryptography (derived from Greek work 'kryptos' meaning hidden and 'graphein' meaning to write) [1] is utilized to encode the content to make it understandable. Cryptography may draw the suspicion of the intruder or third party towards the content that is in encoded. Steganography is the craftsmanship and exploration of composing concealed messages in such a way that nobody, aside from the sender end expected beneficiary, suspects the presence of the message, a type of security without knowledge of its presence. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write" [2]. Steganography can be categorized based on the kind of media it utilizes to hide the data.

Text Steganography: It conceals the text behind some other text file. It is toughest type of steganography as the repetitive measure of text to hide the secret message is rare in text files.

Image Steganography: This type hides text or an image inside another text. It is the most frequently used strategy due to the restriction of the Human Eye.

Audio Steganography: Audio Steganography is a method used to transmit hidden data by adjusting a sound sign in an undetectable way. It is the science of concealing some secret text or audio data in a host message [3]. The host message before applying steganography and stego message after steganography have the same attributes.

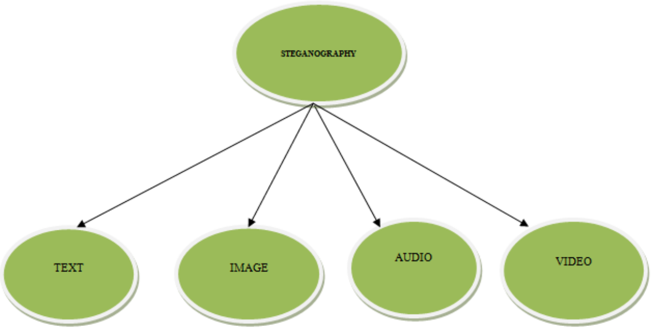


Figure1 Types of Steganography

Video Steganography: Video Steganography is the procedure of concealing some secret data inside a video. The expansion of this data to the video is not conspicuous by the human eye as the change of a pixel color is negligible [3].

1.1 Cryptography

Cryptography, a word with Greek origin means "secrete writing", cryptography is the practice and study of technique for secure communication in presence of 3rd parties communication with security so that unknown person neither access nor modify any data [29].

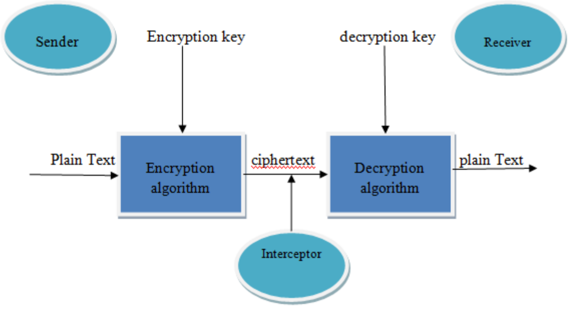


Figure 2 Cryptography

Basic Terms Used In Cryptography -

Encryption - The process of Encoding Plain Text message into cipher text message is called as Encryption.

Decryption - The reverse process of transforming cipher Text message back to plain text message is called Decryption.

Plain text - The original message, before being transformed is called plain text in the form of alphabet, numeric specific symbol [30].

Cipher text- After the message is transformed; it is called cipher text [30].

Key - Some critical information used by the cipher, known only to the sender & receiver.

1.2 SHA Function

In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long.

SHA-1 produces a message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.

1.3 MD5 algorithm

MD5, and additionally MD2 and MD4, takes after a plan standard proposed by Merkle and Damagard. Its essential thought is to do hash in a piece shrewd mode. In a word, MD5 comprises of two phases: cushioning stage and pressure stage. In the cushioning stage, some additional bits (1 to 512bits) are annexed to the information message. The outcome bits is harmonious to 448 mod 512. At that point the length of the underlying message is changed to a 64-bit paired string(if the length is more noteworthy than 264, the lower 64-bit is utilized) and this 64 bits is added to the tail of the message as well. So the cushioning stage closes with a bit stream that comprises of at least one 512-piece squares. In the pressure stage, a pressure work is utilized on each 512-piece square and creates a 128-piece yield. The yield is constantly engaged with the computation of next round.

We start by assuming that we have a b-bit message as information, and that we wish to discover its message process. Here b is a subjective nonnegative whole number; b might be zero, it require not be a various of eight, and it might be self-assertively expansive. We envision the bits of the message recorded as takes after:

m_0 m_1 ... m_{b-1}

The accompanying five stages are performed to process the message process of the message.

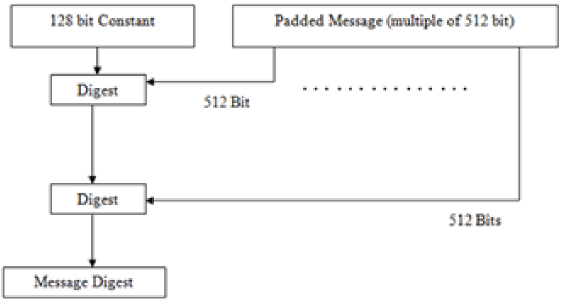


Figure 3 Message function

II. LITERATURE SURVEY

In our dissertation we have take for study the following base papers,

Mohit Sharma [6] author has proposed the secure image transfer concept, for hiding the text message in the image.

Motivation :From this paper we have inspired regarding the concept of the image stegnography , that is , hiding the text in the images as well as the author also introduced the unique concept of the secure file transfer of the images.

AmmadUl Islam [7] author has proposed the concept of image stegnographybased on most significant bits (MSB) of image pixels . This concept we have utilized and some whatextended in our dissertation.

Motivation :From this we have modified our functions of the embedding and extracting the text in the images and audio using the concept of the MSB.

Imran SarwarBajwa [8] concept of hash map for the validating the authenticity of the images we have learned from this paper.

Motivation: From this we got the concept of the using the MD5 hash for getting the authenticating the validity of the images. The hash of the image or audio is send as text message and the received audio or image hash is generated at the receiver end , if both are found same then the image or audio is considered as proper i.e. not modified in the communication path.

Biometrics Based Key Generation using Diffie Hellman Key Exchange for Enhanced Security Mechanism by M.S.Durairajan1, Dr.R. Saravanan

Shared key is the major constraint established by Diffie Hellman Algorithm for two parties without the prior knowledge of each other over insecure communication channel. This algorithm generates the shared key with the help of receiver's public key and sender's private key. This research paper deals with the usage of finger print as the private key for generating the shared key for enhanced security. Using this paper we have used the Diffie Hellman Algorithm in our proposed dissertation

A secure image encryption algorithm based on chaotic maps and SHA-3

In this paper, a chaotic image encryption algorithm is suggested combining with double chaotic maps, SHA-3 (Secure Hash Algorithm-3), and auto-updating system. To shuffle pixel positions, a matrix having same size of the plain-image is generated dependent on the plain-image in stage of permutation. Then, SHA-3 is taken to calculate its hash values used to produce control parameter and initial condition of Logistic map. After that, total permutation is implemented for row and column to exchange pixels, where auto-updating systems are established by different images acting like one-time pad. Furthermore, 3D chaotic cat map is employed to enlarge key space in diffusion process

"Blowfish Algorithm by Josef Steinberger , and KarelJežek blowfish

In this paper the author has discussed Blowfish algorithm, that it is a variable-length key block cipher. And in this he have described in details the working of the blowfish algorithm and applications where the blowfish algorithm is used.For this paper we get the idea regarding the process which is adapted in the encryption and decryption using the blowfish algorithm. The information which we get from this paper are as follows ,the key size which is used for encryption and in the decryption process and rounds which are performed in the data encryption and final output which we get from that. From this paper we have derived the concept of the blowfish algorithm.

III. PROBLEM STATEMENT

Data in transit Those three words are at the heart of business in the 21st century and the rise the of the secure managed file transfer. Companies function by sending, receiving and sharing information, often in very large files, and often in huge numbers of files in batch transactions. Files have to move quickly, reliably and securely.

- The unencrypted file can be accessed by people other than the intended recipient.
- The file traverses an unsecured communication medium that is outside your infrastructure or control.
- There is no way to know if the file integrity is intact if, for example, the file transfer process aborts before it is completed.

IV. PROPOSED CONCEPT

We have proposed a secured File sharing and the message transferring system in which the message combination is done only between the registered users.

The project flow consists of following

1. User Validation

In the user validation, we will select the photo of the user1 and user 2 involved in the sending process. The photos are then validated in the user's databases and the username is fetched. After that using the blowfish encryption algorithms the image are encrypted and send. A long with that a unique transaction key and encryption key is stored in database. Encryption key will act us key to encrypt images.

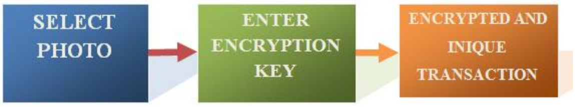


Figure 4: Validation Photo

2. Message Exchange

This process is divided in two parts.

(a) User Validation (b) Message Sending

A. User Validation: Firstly, we will enter the transaction key and key for encrypting image. The entries are validated from databases and then images are decrypted and shown on screen, then only we can proceed to message sending step.

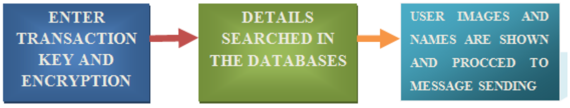

ENTER TRANSACTION KEY AND ENCRYPTION
DETAILS SEARCHED IN THE DATABASES
USER IMAGES AND NAMES ARE SHOWN AND PROCCED TO MESSAGE SENDING

Figure 5: Message sending

B. Message Sending: Now finger prints are input and unique random number an basis of finger print is generated and audio message containing the hidden message will be send.

The message which is send after validation of the users is the audio message which contains the text hidden in it.

The module of the systems is divided into the following parts,

Description:

1. Registration:

-To access the core system, user first need to register themselves by providing required details.

2. Login:

-After registration, user may login into the system.

3. Algorithm Selection:

-Here, user will select the algorithm such as DES (Data Encryption Standard), AES (Advance Encryption Standard) or LSB (Least Significant Bit) for encrypting data into image file.

4. Image Selection/Audio Selection

-Here, User selects an image/audio for sending a secret message. In some case where the encrypted image is sent then the step 5-6 are skipped and a new step of decryption of the image will be introduced.

5. Entering Text:

-Here, User enter/inputs the text that is to be hidden in the image.

6. Setting Password and Encrypting the Data:

-User sets a password and use the encryption technique to encrypt the data.

7. Sharing:

-After hiding the text with the encryption technique, user saves the image a then sends it to the other party i.e. Receiver.

4.1 Algorithm for the Image Encryption

The algorithm for the image encryption is as follows:

Step 1: Read Image file to be encrypted
Step 2: Check for the Image Extension and valid then load the image.
Step 3: Load the Key
Step 4: Convert the image file to binary
Step 5: Encrypt the using the key.
Step 6: Store the Encrypted Image on the Hard disk.

4.2 Algorithm of Decrypting Image

The algorithm of decrypting the image is as follows:

Step 1: Read Image file to be decrypted
Step 2: Check for the Image Extension and valid then load the image.
Step 3: Load the Key
Step 4: Convert the image file to binary
Step 5: Decrypt the using the key.
Step 6: Store the Decrypted Image on the Hard disk

Produce a secret key to encode and to unscramble the data. The DESCryptoServiceProvider depends on a symmetric encryption calculation. The symmetric encryption requires a key and an introduction vector (IV) to encode the data. To unscramble the data, you should have a similar key and a similar IV. You should likewise utilize a similar encryption calculation. You can produce the keys by utilizing both of the accompanying methods:

• Method 1 You can prompt the user for a password. Then, use the password as the key and the IV.

• Method 2 When you create a new instance of the symmetric cryptographic classes, a new key and IV are automatically created for the session.

4.4 Algorithm for Embedding Of Data

The algorithm for embedding of data is as follows:

1. Input the Audio File
2. Input the Text File or Text to be Hidden
3. Input the Key File Used for the Encryption Purpose (Same Key file will be used for Decryption purpose)
4. In the Embedded process first the chunk of wave stream of the audio files are obtained in order to count the number of samples required for embedding the data , if the samples obtained is not sufficient then the error message is generated. Then the source audio stream and destination audio stream are opened (destination audio is the new audio file which get created after the embedding process). Then the message and key are embedded bit by bit with the carrier audio.
5. Finally, we can get the audio with hidden data

4.3 Algorithm for Extracting of Data

The algorithm for extracting of data is as follows:

1. Input the Audio File
2. Input the Text File which will store the extracted data.
3. Input the Key File Used for the Decryption Purpose (Same Key file will be used for Encryption purpose)
4. First the carrier wave file is extracted for the provided audio file, the message is extracted from the audio file using the key file which is provided as input and then a new file stream is obtained in order to write the extracted data into the new destination file.
5. Finally, this data convertedinto original secrete data

V. IMPLEMENTATION

The proposed algorithm is executed in Visual Studio 2010 and SQL Server Express Edition 2008.To run the above programming the required equipment are X86 processor 1 GHz or more of at least 1 GB of RAM.

Presently the part takes after with clarification of execution of algorithm with the assistance of screenshots of my work I have taken amid my viable work.

5.1 Screen Shots of Implementation

The screenshots at various phases of implementation are shown below.

5.1.1. Main Screen

This is the main screen or in other works we can say it is the control panel of our work. Here the Menu driven interface is created in order to select the options related to our work.

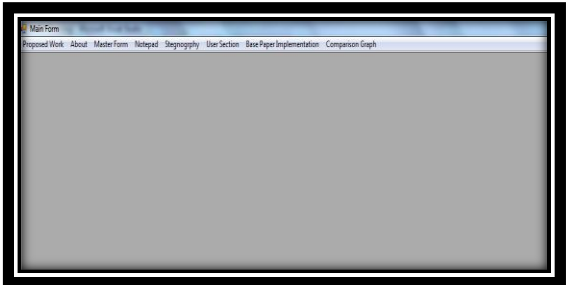
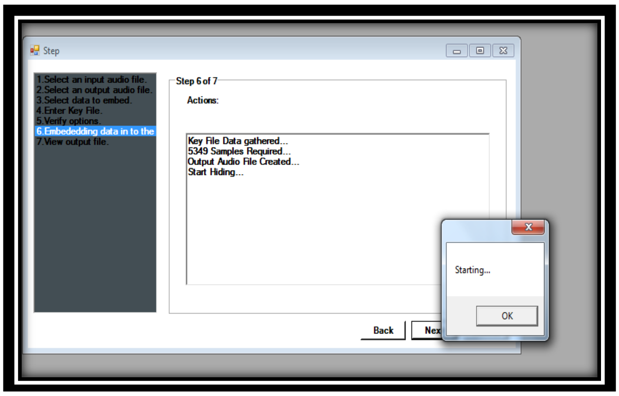


Figure 6 Main Screen

Proposed Work Menu (Audio Steganography)

Figure 7 Proposed Work Menu

In the next step as show in the Fig 8, when we click on the start button the encryption and the embedding process will start.

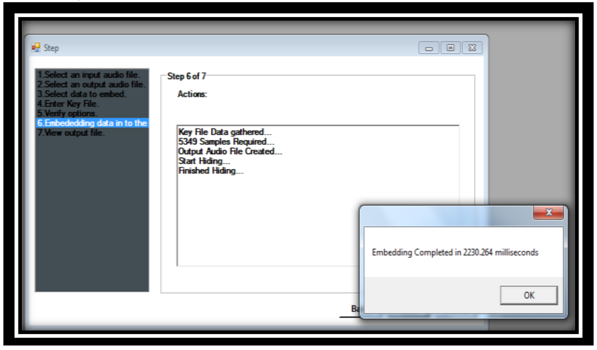


```
Key File Data gathered...
5349 Samples Required...
Output Audio File Created...
Start Hiding...
```

Starting...

Figure 8 Starting the Embedding Encryption Process

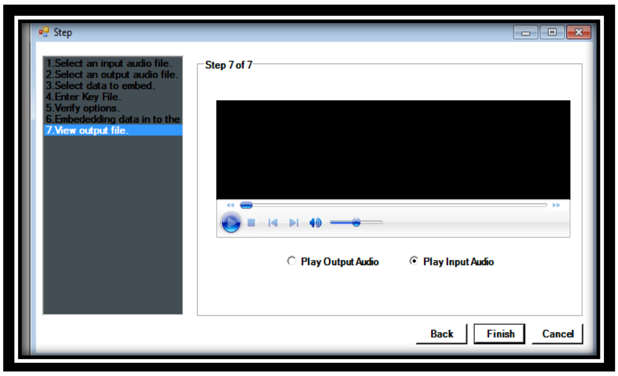
Fig 9 will show the actual time consumed in the process of embedding of text in the carrier audio.



```
Key File Data gathered...
5349 Samples Required...
Output Audio File Created...
Start Hiding...
Finished Hiding...
```

Embedding Completed in 2230.264 milliseconds

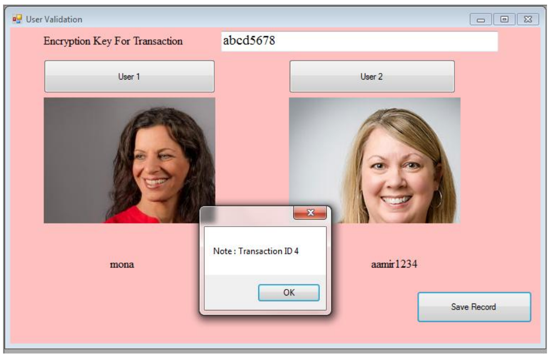
Figure 9 Finished Embedding process



○ Play Output Audio ● Play Input Audio

Figure 10 Output Resultant File

In fig 11 the user images are supplied with the encryption key to encrypt the image , and after that the valid and unique transaction key is generated , this done in order to validate the users involved in the transaction.


User Validation

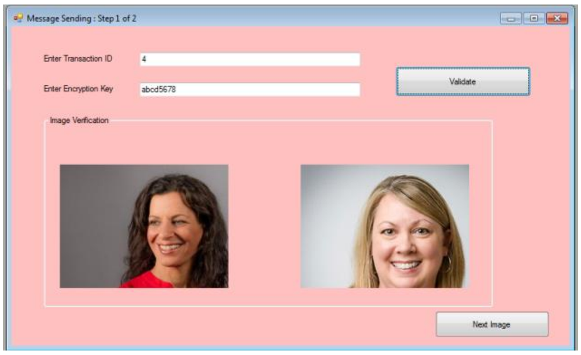
Encryption Key For Transaction abcd5678

mona

aamir1234

Note : Transaction ID 4

Figure 11 Validating the User


Message Sending : Step 1 of 2

Enter Transaction ID 4

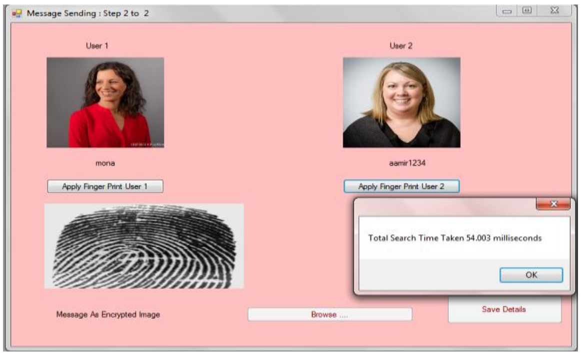
Enter Encryption Key abcd5678

Image Verfication

Figure 12 Encrypted Audio Message sending step 1

In fig 12 , the user have to first supply the valid transaction id and then the encryption key after that the user participating in the transaction are shown and after than the next step of the message sending will appear in the fig13 .

In fig 13 , in order to cross validate the user the finger print are supplied and the finger print validation is done with the help of the MD5 Hash.


Message Sending : Step 2 to 2

User 1 mona

User 2 aamir1234

Total Search Time Taken 54.003 milliseconds

Message As Encrypted Image

Figure 13 Finger Print validation

And after the finger print validation is done then the message is allowed to send. And the message is again an encrypted image which is to be send to the receiver.

VI. CONCLUSION AND FUTURE WORK

In this, the audio steganography is implemented, where the audio message can securely carry the text. The proposed work provides secure secret communication among sender and receiver, it ensures that embedded data remains inviolate & recoverable, also, authenticating the sender and receiver using Blowfish encryption and SHA algorithms while maintaining secrecy. The data which is hidden cannot be transmitted without prior user verification and it can not be easily accessed by common audio manipulation techniques.

REFERENCES

[1] H. Liu, J. Liu, R. Hu, X. Yan and S. Wan, "Adaptive Audio Steganography Scheme Based on Wavelet Packet Energy," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp. 26-31.

[2] J. S. Lamba, K. Sachdeva, V. Sinha and N. Singh, "Differential pulse code modulation in audio steganography," 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), Mysuru, 2016, pp. 131-135.

[3] A. Devi and K. B. ShivaKumar, "Novel Audio Steganography Technique for ECG Signals in Point of Care Systems (NASTPOCS)," 2016 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, 2016, pp. 101-106.

[4] M. Rana and F. B. Kunwar, "A temporal domain audio steganography technique using genetic algorithm," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 3141-3146.

[5] B. Datta, P. Pal and S. K. Bandyopadhyay, "Robust multi layer audio steganography," 2015 Annual IEEE India Conference (INDICON), New Delhi, 2015, pp. 1-6.

[6] M. Tayel, A. Gamal and H. Shawky, "A proposed implementation method of an audio steganography technique," 2016 18th International Conference on Advanced Communication Technology (ICACT),Pyeongchang, 2016, pp. 180-184.

[7] Fabian Monrose, Michael K. Reiter, Qi Li , Susanne Wetzel, "Cryptographic Key Generation from Voice", In Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001.

[8] Neha Rani and Jyoti Chaudhary, "Text Steganography Techniques: A Review", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 7- july 2013

[9] Swati Gupta and Deepti Gupta, "Text - Steganography: Review Study & Comparative Analysis", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011

[10] ChintanDhanani and Krunal Panchal, "Steganography using web documents as a carrier: A Survey", International Journal of Engineering Development and Research (IJEDR), ISSN: 2321-9939, 2013