International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 5, May 2016)

DWT Colour Image Stenography Based Voice Biometric Authentication System

Mehdi Hafeez Lohar
M.Tech (DCN)
Dept. Of Electronics & Communication
PACE, Mangalore Karnataka India
Mehdihafeez123@gmail.com

Mohammad Hussain
Assistant professor
Dept. Of Electronics & Communication
PACE, Mangalore Karnataka India
Hussain_mtech@pace.edu.in

Abdullah Gubbi
Professor & HOD
Dept. Of Electronics & Communication
PACE, Mangalore Karnataka India
Hod_ece@pace.edu.in

***Abstract*— Voice recognition is a process of identifying the identity of an unknown speaker on the basis of individual information that contain in the speech signal. Voice recognition is one of the biometric technologies used in a security system to reduce cases of fraud and traits. Voice biometric is an easy and cost effective biometric technique which requires minimalistic hardware and software complexity. General voice biometric needs a voice phrase by user which is processed with Mel Filter and Vector Quantized features are extracted. Vector quantization reduces the codebook size but decreases the accuracy of recognition. Therefore we propose a voice biometric system where voice file's non quantized code books are matched with spoken phrase. In order to ensure security to such direct voice sample we embed the voice file in a randomly selected image using DWT technique. Imposters are exposed to only images and are unaware of the voice files. We show that the technique produces better efficiency in comparison to VQ based technique.**

***Index Terms*— Wireless Sensor Network, Matlab, steganography, etc.**

I. INTRODUCTION

Many reversible and irreversible methods for template security have been proposed. But, unlike other biometric forms like face and fingerprint biometric, voices are easy to imitate. Therefore mere cryptographic use for securing voice templates are not sufficient.

Therefore we change the mode of processing by first storing the voice itself behind an image to change the nature of file.

Templates from training instances are generated at the run time by first extracting the voices from image followed by template extraction. As templates are extracted and matched at the run time, possibility of tempering is reduced significantly.

Contributions of the project

General voice biometric needs a voice phrase by user which is processed with Mel Filter and Vector Quantized features are extracted. Vector quantization reduces the codebook size but decreases the accuracy of recognition. Therefore we propose a voice biometric system where voice file's non quantized code books are matched with spoken phrase. In order to ensure security to such direct voice sample we embed the voice file in a randomly selected image using DWT technique. Imposters are exposed to only images and are unaware of the voice files. We show that the technique produces better efficiency in comparison to VQ based technique.

II. PROBLEM STATEMENT

There are certain issues related to biometric system and biometric data. Biometric systems are vulnerable to attacks, which can decrease their security. As template is stored in database, if the security of stored templates is compromised, the attacker can gain unauthorized access. The stolen templates can also be used for other unintended purposes, e.g. performing unauthorized credit-card transactions or accessing health related records.

We can protect the biometric data and template by using cryptography, steganography and watermarking.

III. LITERATURE SURVEY

The literature review shows the work that has already been done on image steganography using different techniques. There are various methods which are applied for secret communication of data. Considerable amount of work has been done for embedding different media's in image, while much research is needed in the field of embedding audio file with in digital images. This can provide maximum security while transferring data. Whereas brief literature review is specified below.

Souvik Bhattacharyya and Gautam Sanyal proposed approach works by converting the gray level image in transform domain using discrete integer wavelet technique through lifting scheme. The aim of this paper is to propose a high-capacity image steganography technique that uses pixel mapping method in integer wavelet domain with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security.

Ammar Abdul-Amer Rashed proposed a companied technique for hiding secret messages (text) based on wavelet transform applying in cover image (a gray level image 8bit) and Huffman encoding. The experimental results show that the algorithm has a high capacity and a good invisibility, Moreover PSNR of stego image shows the better results the PSNR above 40 dB, the proposal system was activated according to attacker noise is addition and JPEG compression application are used without detection the secret message.

S. K. Muttoo and Sushil Kumar proposed a stenographic algorithm based on wavelet transforms. The algorithm first

uses the Best T-codes to encode the message before embedding into a cover image.

Saddaf Rubab and Dr. M. Younus presented a new devised algorithm to hide text in any colored image of any size using Huffman encryption and 2D Wavelet Transform. The subject algorithm also proved secure as Huffman table is required to decode the information.

Manjunatha Reddy and Raja proposed High Capacity and Security Steganography using discrete wavelet transform (HCSSD). The wavelet coefficients of both the cover and payload are fused into single image using embedding strength parameters alpha and beta. The cover and payload are preprocessed to reduce the pixel range to ensure the payload is recovered accurately at the destination. It is observed that the capacity and security is increased with acceptable PSNR in the proposed algorithm compared to the existing algorithms.

Lalitha.G et al., proposed a technique for the simultaneous transmission of multiple data securely. They took an advantage of less space required for storing an image than that of a wav file. The proposed technique brings down the required channel capacity to transfer secret data in real time systems besides improving robustness.

Elham Ghasemi et al., proposed the application of Wavelet Transform and Genetic Algorithm in a novel steganography scheme. We employ a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image.

Kirith saroha and Pradeep kumar singh proposed a new steganography method for embedding an image in an Audio file. Emphasis will be on the proposed scheme of image hiding in audio and its comparison with simple Least Significant Bit insertion method of data hiding in audio. It is an attempt to find a method that uses an audio file as a cover media to hide an image without making noticeable changes to the file structure and contents of the audio file. The proposed scheme is based on Least Significant Bit insertion method as it has been already proved that modification of LSB creates a minimal change in the audio file format.

Akram M. Zeki et al., provided analysis on steganographic techniques and undertake an experiment using five Steganographic software in order to explore their capabilities. Benchmarking tool for identifying different performance aspects of the Steganographic techniques and Steganographic software like visual quality, performance indices, memory requirement and the evaluation of the maximum capacity for each software under this study.

Jayaram P et al., made a survey on audio steganography. They proposed that Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file. This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

Md. Shafakhatullah Khan et al., proposed a new approach which is sophisticated for concealing the data. They describes how the data is secured form the intruders even though they trace the audio file which contains the confidential data. The basic idea is to provide an optimized method for concealing the private data from intruders and sent to the destination in a safer and secure manner. It is an enhancement of spread spectrum audio data hiding methods.

Wei Qin Cheng et al., proposed a robust audio steganography. They implemented a simple Dynamic Linked Library [DLL] by using managed C++ and Microsoft .NET framework. It is implemented by Direct Sequence Spread Spectrum [DSSS] method on data block base.

Reference paper thirteen and fourteen provides an overview of voice properties and information about biometrics and speech technology. The information needed for the methodology, which involves Mel Frequency Cepstrum Coefficients technique for Feature extraction process and Vector Quantization technique for Feature matching process, is taken from and . Feature extraction is the process that extracts a small amount of data from the voice signal that can later be used to represent the speaker. Feature matching involves the actual procedure to verify the speaker by comparing extracted features from his/her voice input with the claimed one which is stored in the database.

M.I.Khalil has discussed the possibility of hiding short audio messages inside the digital image. His proposed approach encrypts the audio message before hiding it into the image. He has used cryptography, steganography, audio message, least significant bit (LSB) method whereas the purpose of steganography is to communicate completely in an undetectable manner. For hiding audio common files like Wave files (wav) and MPEG layer-3 files (mp3) are used. Size of audio file to be hidden depends on the size of image file. Regardless of the selected audio file LSB insertion of message bit into the image is applied. LSB is used due to its simplicity of embedding directly into the LSB plane of cover image. Changing LSB bits does not result in human perceptible difference because the change is very rare. For a human eye the final image will look identical to the cover image.

Hemalatha S,, U. Dinesh Acharya, Renuka A proposed a technique where image steganography is used to hide audio signal in image in the transform domain using wavelet transform. The audio signal in any format (MP3 or WAV or any other type) is encrypted and carried by the image without revealing the existence to anybody. When the secret information is hidden in the carrier the result is the stego signal. In this work, the results show good quality stego signal and the stego signal is analyzed for different attacks. It is found that the technique is robust and it can withstand the attacks. The quality of the stego image is measured by Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), and Universal Image Quality Index (UIQI). The quality of extracted secret audio signal is measured by Signal to Noise Ratio (SNR), Squared Pearson Correlation Coefficient (SPCC). The results show good values for these metrics.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 5, May 2016)

IV. PROPOSED SYSTEM

The new idea has been proposed for the security of secret information and parties as well. The Main goal of this method is to develop an efficient security system for the protection of confidential data during the transformation process.

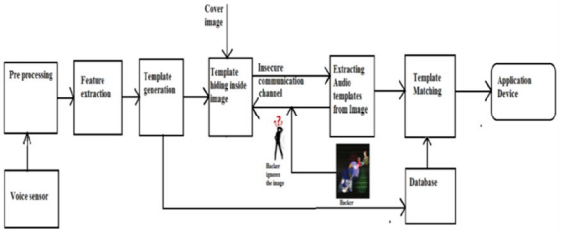

Figure 1: Block diagram of proposed system

The above Block diagram shows the actual flow of the project. The main goal of voice recognition system is to verify whether the speaker is who he/she claims to be and whether he has spoken his key phrase or not. The system processes voice signal of the user, which is given as input and finds the Mel Frequency Cepstrum Coefficients. Then it generates a template, which is called a codebook, an array of acoustic vectors. In the enrollment phase the user codebook is saved in the system. In the verification phase the user codebook is compared against the claimed user's actual codebook, which is stored in the system during the enrollment phase. If the difference is below the threshold value the user is authenticated else the user is not authenticated.

Before the transmission of the claimed user codebook during the testing phase the codebooks/templates are inserted inside the image using a technique called stegnograpgy. The cover object used to hide secret voice is color image. Hence the imposter will remain unaware of those voice and he will see only an image.

MFCC approach for voice feature extraction

Feature extraction process is carried out as extraction of significant frequency components from voice file. MFCC function is liked a mimic the behavior of the human ear. MFCC process produces a number of coefficients that identify the processed speech and these parameters are used in speaker recognition or in speaker verification systems. There are few steps need to be taken in MFCC process: framing, hamming window, Fast Fourier Transform (FFT), mel frequency wrapping, ceptrum and MFCC. Each step has its own function and analysis.

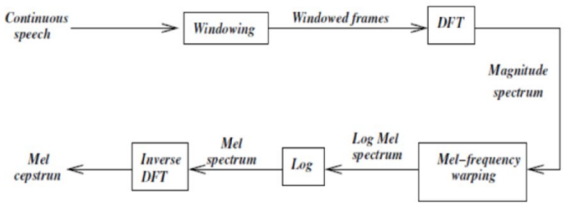

Figure 2: MFCC processor

Feature extraction process is carried out as extraction of significant frequency components from voice file. MFCC function is liked a mimic the behavior of the human ear. MFCC process produces a number of coefficients that identify the processed speech and these parameters are used in speaker recognition or in speaker verification systems. There are few steps need to be taken in MFCC process: framing, hamming window, Fast Fourier Transform (FFT), mel frequency wrapping, ceptrum and MFCC. Each step has its own function and analysis

Frame Blocking

Frame blocking or framing is used after the continuous voice is captured and blocked into frame of N samples, through adjacent frames being divided by M (M<N). Typically in this section, speech sample in boxes within the range 20 ms to 40 ms [20]. The purpose of frame blocking is to ensure the speech signal in a short period of time. The characteristic of speech signal in a short period of time shows the speech signal nearly in stationary which is it easy to analyze. A long period of time of speech signal may cause the characteristic of speech signal change. Figure 3.2 shows a sample of a speech signal of unknown speaker.

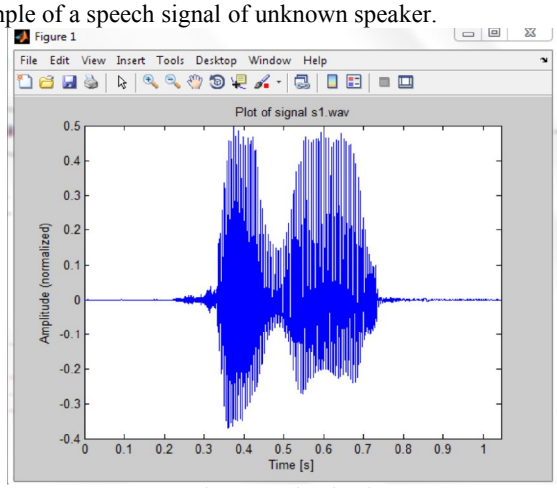

Figure 3: Voice signal

Windowing

The next step is windowing where each individual frame will through this process as to minimize the signal discontinuities o speech signal at the beginning and at the end of the frame. Besides, it also to minimize the spectral distortion by using the window to atenuate to zero value at the beginning and the end of the frame [17]. The window can be defined in equation (3.1).

$$W(n) = 0 \le n \le N-1$$ Where N is the number samples in each frame.

V. ALGORITHM FOR DETECTION OF MALICIOUS NODES

Encoding Algorithm

1. Load the cover Image
2. Perform DWT2 to obtain the coefficients.
3. Converting the coefficients to a single row
4. Making adjustments of the coefficients values.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 5, May 2016)

5. Reading the audio file and calculating the size of the audio file which is a secret message.
6. Resize the size of the secret image to fit inside Image.
7. Store the audio length inside cover image in CV, CH, and Cd.
8. Apply Inverse DWT to get the original cover image which is a stegno image.

Decoding Algorithm.

1. Execute DWT on stegno image at the receiver side.
2. Recognize the high pixel density areas of the stegno image.
3. Get Standardized audio.
4. Obtain the hidden voice components from the image.
5. Send the voice to matching phase for recognition.

VI. RESULTS

In this project we suggest a method for voice biometric template safety by hiding recorded users vocal sound file behind the image. There are many variants of hybrid steganography but the proposed work of DWT based image steganography followed by spectrum based audio steganography is finest combination and best suitable for the security of voice biometric authentication system.

In order to do so, In this work In the encoding stage firstly we have taken a cover image randomly which is a color image of size 512x512 for hiding the trained file of a user. This color Image is decomposed through Haar wavelet to yield multi scale image. The voice feature extraction is done by using Mel frequency cepstrum coffiencient. The voice features are concealed behind the image by keeping normalized audio bits behind wavelet image bits. Then Inverse transform is applied to get stegno image which is same as cover image.

In the decoding stage the cover image is converted through wavelet. First dense regions are identified. Then normalized voice data is mined and remapped to actual real scale. The voice data is then passed through the matching process where voice file is matched with the claimed user's voice and authentication is provided based on the matching result.

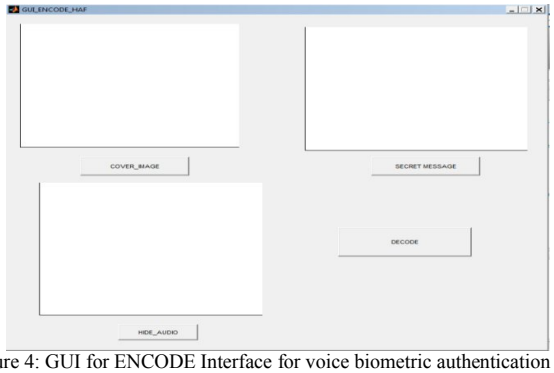

Figure 4: GUI for ENCODE Interface for voice biometric authentication and protection scheme

The GUI interface for voice biometric authentication and protection scheme has two parts. First one is ENCODE GUI interface and second is DECODE GUI interface. ENCODE GUI interface consists of three push buttons as shown in the fig 6.1.They are named as cover image to select a cover image, secret message to select the secret voice message which we are going to hide inside the image, hide audio button which hides the secret voice inside the image and a decode push button.

As shown in fig 6.2 upon clicking on the cover image push button a cover image being selected which is a color image of size 512x512 pixels.

Fig shows the secret voice message is being selected upon clicking of secret message push button.

Once the secret voice message is selected the next step is to hide the secret message inside cover image to obtain a stegno image. The process in shown in fig 6.4.

After hiding the secret message the decode push button is clicked which is a linker between encode GUI and decode GUI. A decode GUI appears on the screen after clicking decode push button.

In decode GUI there are three push buttons they are as load stegno image, Extract audio, audio recognition and a display scrren,as shown in fig 6.5.

In the decoding GUI, The stegno image is loaded and the secret audio is extracted from the stegno image after pressing load stegno push button and extract audio push button. Then audio recognition push button displays the message as the person is authenticated or not authenticated.as shown in fig 6.6 and fig 6.7.

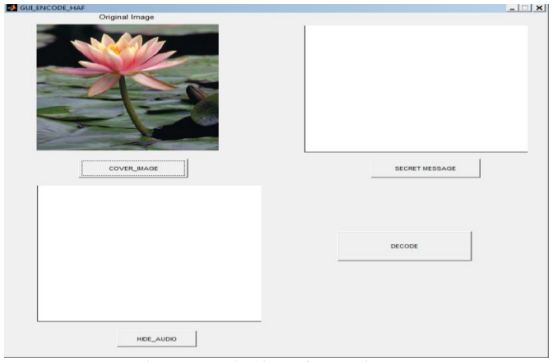

Figure 5: Selection of cover image.

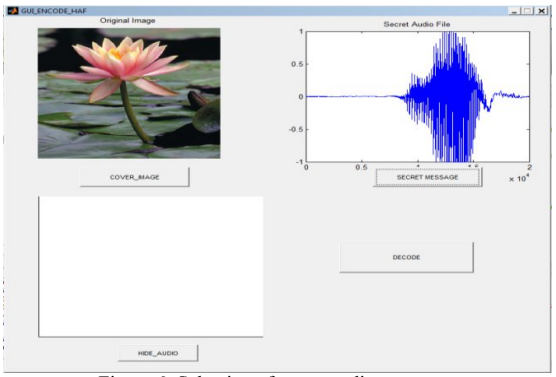

Figure 6: Selection of secret audio message.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 5, May 2016)

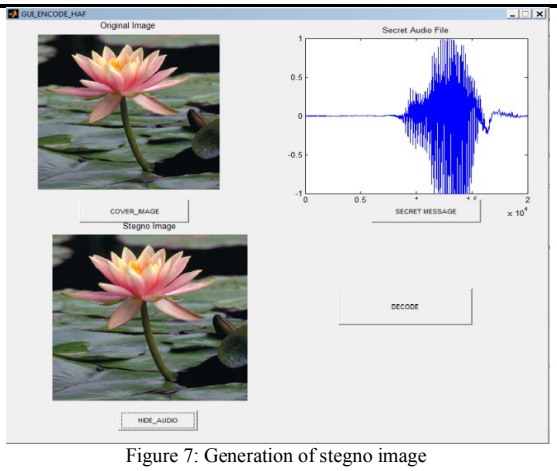

Figure 7: Generation of stegno image

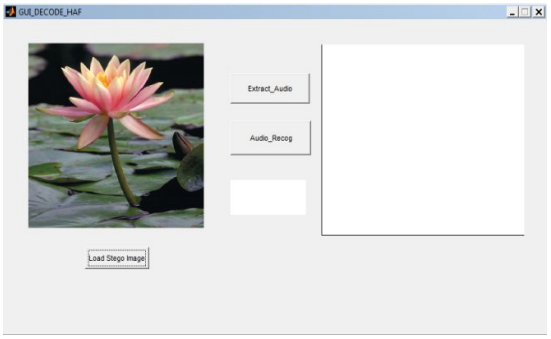

Figure 8: Loading of stegno image in DECODE GUI

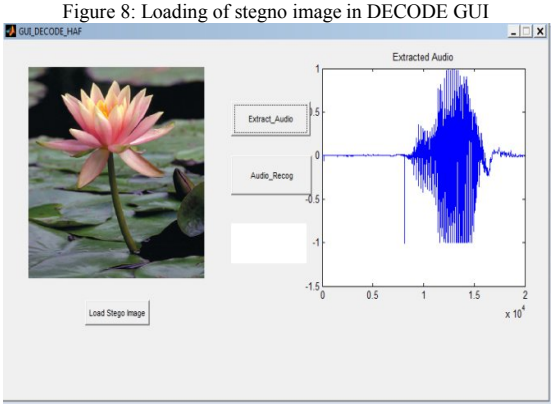

Figure 9: Extraction of secret audio message from the stegno image

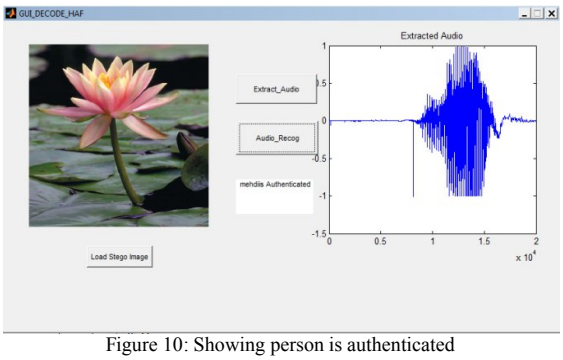

Figure 10: Showing person is authenticated

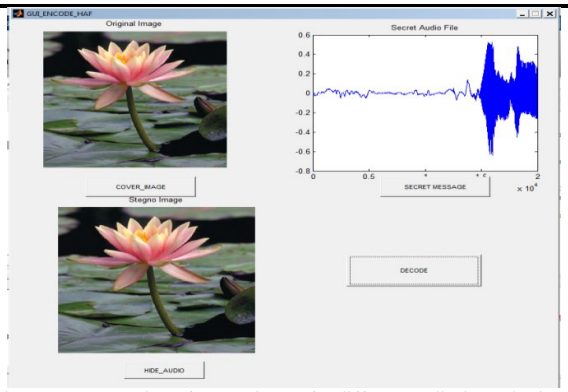

Figure 11: Generation of stegno image for different audio /unauthorized person

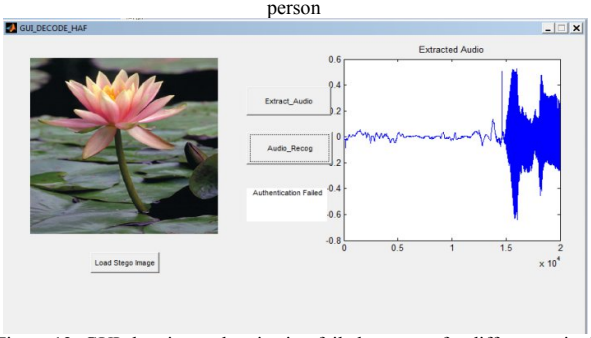

Figure 12: GUI showing authentication failed message for different voice/ unauthorized person

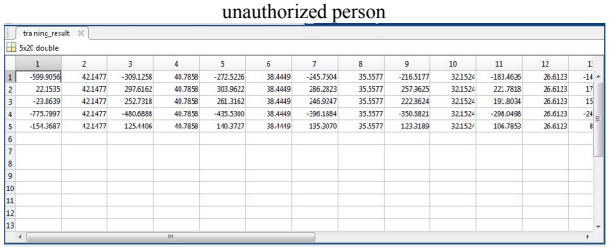

Figure 13: Database trained with five user's voice samples showing their corresponding coefficient values from column 1 to 20.

VII. APPLICATIONS

Applications of voice biometric authentication system

- **Access control**
  - Physical facilities
  - Data and data networks, computers, cell phones.
- **Transaction authentication**
  - Telephone transactions
  - Home banking or online banking.
  - Fraud identification.
- **Monitoring**
  - Remote time and attendance logging
  - Home parole verification
- **Information retrieval**
  - Customer info for call centers
  - Audio indexing (speech skimming device)
  - Personalization
- **Forensics**
  - Voice sample matching

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 3, Issue 5, May 2016)

VIII. CONCLUSION

Safety plays an important part in all phases of Biometric. Equally the technology develops its limits in the optimistic way, so do the opposite engineering of it. Info safety has been of main focus these days and plays a main part in way of its complexity. One way of providing data security is by means of steganography.

The suggested work is one of the newest progresses achieved in the field of biometric safety. In this Effort a user's vocal sound data known as the payload is inserted into an image which is so-called the cover image. For an all-purpose outlook it seems as a simple Image file.

A query now rises as to how this will be safe as one can simply find the alterations in the image. The BPP study shows that the Bits per pixel of the method is very high. Hence image alterations are least.

Finally we conclude that performance measurement of the recognition accuracy shows that the proposed scheme yields a voice recognition accuracy y of 88% with only .3% incorrect recognition rate in contrast to VQ based technique which produces an overall accuracy of 81% with 6% FA.

REFERENCES

[1] K B Shiva Kumar ET. al. ―Bit length replacement steganography based on DCT coefficients‖ / International Journal of Engineering Science and Technology. Vol. 2(8), 2010, 3561-3570

[2] K B Shiva Kumar et. al ―Hybrid Domain in LSB Steganography‖ International Journal of Computer Applications (0975 – 8887). Volume 19– No.7, April 2011

[3] K B Shiva Kumar et. al ―Steganography Based on Payload Transformation‖ IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011. ISSN (Online): 1694-0814. www.IJCSI.org

[4] Saddaf Rubab, Dr. M. Younus. ―Improved Image Steganography Technique for Colored Images using Huffman Encoding with Symlet Wavelets‖ IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012 ISSN (Online): 1694-0814‖.

[5] Akram M. Zeki, Adamu A. Ibrahim And Azizah A. Manaf, ―Steganographic Software: Analysis and Implementation‖ International Journal Of Computers And Communications Issue 1, Volume 6, 2012

[6] S. K. Muttoo and Sushil Kumar, ―Robust Source Coding Steganographic Technique Using Wavelet Transforms‖ BVICAM's International Journal of Information Technology.

[7] Kriti Saroha and Pradeep Kumar Singh ―A Variant of LSB Steganography for Hiding Images in Audio‖. International Journal of Computer Applications (0975 – 8887) Volume 11– No.6, December 2

[8] Lalitha.G et al. / International Journal on Computer Science and Engineering (IJCSE), ―Secure Transmission of Compound Information Using Image Steganography‖

[9] Md. Shafakhatullah Khan et al. ―An Optimized Method for Concealing Data using Audio Steganography‖ International Journal of Computer Applications (0975 – 8887) Volume 33– No.4, November 2011

[10] Pradeep Kumar Singh et. al ―Enhancement of LSB based Steganography for Hiding Image in Audio‖. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1652-1658

[11] Jayaram et al. ―Information Hiding Using Audio Steganography –A Survey‖The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

[12] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi. ― High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm‖. Proceedings of the international multiconference of engineers and computer scientists 2011 volI

[13] Minh N.Do, *An Automatic speaker Recognition System*, Audio Visual Communications Laboratory, Swiss Federal Institute of Technology, Lausanne, Switzarland.

[14] J.W. Cooley and J.W. Tukey, *An algorithm for the machine calculation of complex Fourier Series*, Mathematics Computation, Vol.19, 1965, pp 297-