Enhancing MultiBiometric System Security at Feature Level Fusion

Gaganpreet Kaur
Research Scholar
Deptt. of CSE,
I.K. Gujral P.T.U, Punjab, India

Dr. Shashi Bhushan
Professor
Deptt. of I.T,
CEC, Landran, Punjab, India

Dr. Dheerendra Singh
Associate Professor
Deptt. of CSE,
CCET, Sector-26, Chd, India

Abstract-Multimodal Biometrics has received attention in the last ages because it is afascinating alternative to traditional authentication systems like passwords etc. Authentication is required when it is necessary to know if a user is who they claim to be. Sometimes the traits are increased due to enhancement in number of users which affect the database and authentication system's performance. Single biometric based systems are excelling as it is very easy and fast system to access the biometric features of a user. However with the introduction of safety measures, more threats are developing too in a parallel manner to the security systems. Ultimately it has become a key point to work on a multimodal biometric system which can not only provide higher degree of security but may also provide the same with 100% accuracy and efficiency. In this paper a prototype for the same has been proposed. The focus is kept on design of a multimodal Biometric system based on tongue, speech and signature recognition. As well as the maximum value observed is to be treated as the best match. In this proposed work higher level of security is added to multi biometric system involving speech, signature and tongue biometrics by use of password technique using the image steganography.

Keywords:Multimodal Biometrics, FNMR, FMR, Correlation coefficient

I. INTRODUCTION

Multi biometrics integrates different biometrics systems for verification in making user identification. This system has advantages to the capabilities of each individual biometrics. Identification (identify) is defined by the one-to-many process of matching submitted Biometric data against all other Biometric reference templates to determine whether it matches any of the templates and to determine the identity of the enrolee whose template matches the Biometric data. Verification (verify) is defined by the process of matching (comparing) a given Biometric data (not stored in a database) with the Biometric reference template (stored in a data- base) of a single user whose identity is being checked to determine whether it matches the enrolee‟s template. For example on a computer system, a unique verification token (with direct correspondence to each username) is intended to verify the identity of a legitimate user. All unimodal biometric systems can be used with combination of other to form a multimodal biometrics. For example

- Speech and signature
- Face and iris
- Fingerprint and hand geometry
- Speech, signature and face

In the proposed system a new multi sensor based system is designed in which speech, signature and tongue of a user will be recognized by a logic-condition based algorithm and an enhanced version of password technique using the image steganography will be adding a higher level of security while dealing with the identification process.

II. LITERATURE REVIEW

A lot of work has been done in the field of biometrics security by the researchers to facilitate the people. Cameron Whitelam et. al. [1]worked on two differentwatermarking and steganography based methods which were applied on different biometrics data. But these methods were introduced for the purpose to enhance the security of biometric templates in the data base from the unauthorized attackers.Vabhive B. Joshi et. al. [2] explained a reversible watermarking technique to make the authentication system more secure based on the biometric logic. As well as which given that watermark reversibility in the proposed method ensured that its presence do not affect native biometric authentication. Emanuele Maiorana et. al. [3] discussed about one other way to give the enhancement in the security of signature templates by applying the cryptosystem on the date base of online signature which show that proposed protected online signature recognize systems which gave the guarantees recognition rates which was totally comparable with those templates which were not secure or which were not protected. So that gave the most reliable signature traits, less affecting the entropy of the employed binary representation which was more deniable to privacy attackers. Mandeep Kaur et. al. [4] introduced the fusion of two different modalities which were speech and signature by which this combination of multimodal increased security and accuracy, yet the complexity of the system increases due to increased number of features extracted out of the multiple samples and was poor in terms of response time as the acquisition time increased. This procedure has shown 95% accurate results and gave minimum false accepted rate and false rejection rate which effect the accuracy of the algorithm. Nagesh Kumar et. al. [5] proposed an efficient multimodal biometric face recognition using speech signal into a new application of plastic surgery. In this technique, speaker identity was correlated with the physiological and behavioural characteristics of the speaker. Seiichi Nakagawa et. al. [6] worked on the combination of Mel Frequency Cepstral Coefficient and phase information. As well as it shown the two different modals which are GMM (Gaussian Mixture Modal) and MFCC (Mel. Frequency capstral

speaker verification rate about 97.3% to 98.6% with only 0.93 equal error rate.

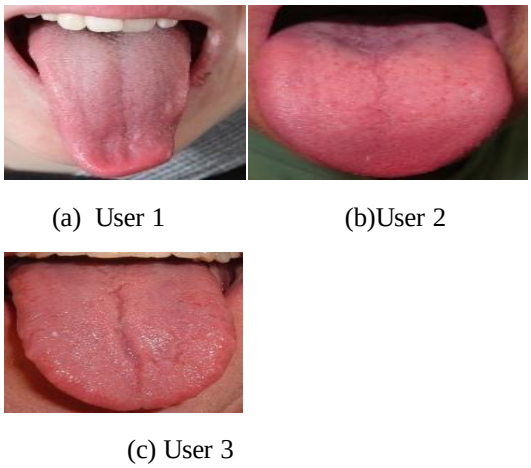
In [7] introduced a feature level fusion in which two different biometric modalities speech and signature were considered. It was an efficient and robust biometric system.

Eshwarappa M.N. et. al. [8] presented the combination of three different modalities of speech and signature and handwriting signatures. This is one of the best combinations which could have been used ever. In this paper it also worked on different classifiers which are for feature extraction using DCT and MFCC and using Z-score normalization. As a result, the identification performance is 100% and verification performances i.e.False Acceptance Rate (FAR) is 0%, and False Rejection Rate (FRR) is 0%.

In [9] the discussion in this paper is about system using Hidden Markov Modals (HMM) extract the data which had been presented which combine information from three different biometrics information in an automatic unsupervised fusion adapting to the local performance of each expert by which a benefit of a approach described is that audio visual training data is not required to tune the fusion process. P.B. Kathe et. al. [10] discussed offline text using scale invariant feature transform descriptor for automated writer recognizer which has methods involving a reduced number of parameters for creation of a robust writer recognition system. As well as in such a case writer identification is been a great arena for development in forensic analysis. In which word segmentation and SIFT are used for feature extraction and the proposed system automated writer recognizer for offline text uses SIFT algorithm to normalize the size of the text. And shown with normalization there are two distances are fused to measure the dissimilarities between two handwriting images.In another work in [11] proposed Encoded Hybrid Digital Watermarking Scheme (EHDWS) to improve image quality which is based on Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and Bose Chaudhuri Hocquenghem (BCH) code. In this they introduced image based watermarking technique to enhance the security of biometric template for singular matrix decomposition which was an Encoded hybrid DWT based watermarking scheme. Proposed framework for watermarking scheme which is based on DWT and SVD transforms with BCH code based authentication.Biometrics systems, components, requirements and performance of biometric systems are well explained by Ross, Jain and Delac [13-15].

III. DATABASE FOR PROPOSED WORK

The very first step is to get the information to be processed. The test images of signaturefrom SVC20EU database and tongue database from [12] were used in work. So, a lot of data was collected from the random population. This data has not only been used for the current research but can also be used in the achievements of future research goals. Second major problem of Speech Signal was solved by getting the speech samples recorded in different slangs from different people. The database was generated in MATLAB in accordance with the information collected from the population and internet as well. Figure 1 shows tongue samples for different users used in work. Table 2 shows test images used in work.



(a) User 1 (b)User 2

(c) User 3

Fig.1 Tongue Image Sample of 3 Different Users

Next step was the acquisition of speech signal corresponding to above three users for the generation of database. The speech signal was recorded using a microphone.

IV. PARAMETERS EXTRACTED FOR SPEECH SIGNATURE AND TONGUE BIOMETRIC SAMPLES

The various parameters for the Signature and Tongue (treating them as an image) and Speech, are calculated as follows:

A. Signature and Tongue Parameters

1) Standard Deviation: It is a measure that is used to quantify the amount of variation or dispersion of a set of data values from mean value. It can be calculated as:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}} \quad ..(1)$$

2) Mean**:-** It is measure of the central tendency either of a probability distribution or of random variable characterized by that distribution. It can be calculated as:

$$\bar{x} = \frac{\sum_{1}^{n} x}{n} \quad ..(2)$$

where n is the number of the iteration (pixels in case of an Image).

3) MSE: Mean Square of a signal can be calculated as:

$$\text{MSE} = \frac{\sum_{m,n}[I_1(m,n) - I_2(m,n)]^2}{m * n} \quad ..(3)$$

4) PSNR: Peak Signal to noise ratio is the ration of signal value of a processed signal to the noise in the same, when defined in concern with an Image. It can be calculated as:

$$\text{PSNR} = 10\log_{10}(R^2 | MSE) \quad ..(4)$$

5) Entropy: It characterizes ones uncertainty about our source of information, and increases for more sources of greater randomness.

B. Speech Parameters

1) Pitch: It is defined as the values of frequency at any particular interval of time. It is measured in Hertz.
2) Tempo: It can be calculated by detecting periodicities from the onset detection curve.
3) Pulse Clarity: It estimates the rhythm clarity indicating the strength of the various high and low frequencies by mir tempo function in MATLAB.
4) Zero Cross: It is a simple estimate of noisiness obtained by calculating the number of times the signal crosses the x-axis.
5) Roll Off: It is the one way of estimation of amount of high frequency in the signal such that criterion fraction of the total energy is contained below that frequency.
6) Spectral Centroid: It is calculated as the weighted mean of the frequencies present in the signal.
7) Spread: This is nothing but the standard deviation of the speech data (Spectrum). Its second central moment called variance is usually given by symbol sigma squared.

V. PROPOSED ALGORITHM& IMPLEMENTATION

Methodology:

Password in the form of (navi%, gunjann& etc.) was embedded onto an image. A 16 bit image was taken for embedding. Least significant steganography method was used for embedding process. During testing phase, user was enquired about password, if it was correct and matched then speech tongue and signature samples were matched with database. If found correct then features of samples were calculated.The parameters like Peak Signal to Noise Ratio (PSNR), Maximum Error and Mean Square Error (MSE) was calculated between the original image and image with the password encoded. The authentication of the results is based on the correlation between biometric features of detected person and those from the database.The test images of signature from SVC20EU database and tongue database from above work are used.The overall procedure of the proposed algorithm can be described as follows:

1. Enter the identity number and password from the user.
2. Match the password with the image with password embedded using bit based steganography (LSB). If match is correct, user is asked to enter the test images of tongue and signature and speech samples else repeat the above process.
3. Calculate various features of signature, tongue and speech.
4. Calculate correlation value of these features to that of stored in database by using

$$R = corr(A, B)$$

where A and B vectors of same size
5. If correlation value =1 then user name is displayed.
7. Fusion of features of speech, signature, and tongue is done using sum rule.
8. Authentication of results and matching with database.

The proposed work was implemented on Matlab 7.11 (R2010b).

VI. RESULTS

The proposed algorithm was tested over large test sets, belonging to different users. The algorithm has produced very enthusiastic results. When the correlation between the two data test image and database data was calculated, the maximum value observed and was to be treated as the best match value and algorithmic results were found to be 100% accurate in all cases.Table 1 for different inputs along with the parameters for various biometrics has been shown below.

Table 1: Comparison of the results of the Accuracy

PARAMETERS	RESULTS
FAR	0.03
FRR	0.05
ACCURACY (%)	99.92

VII. CONCLUSION AND FUTURE WORK

In this work algorithm has been proposed and implemented for identification of a user based on biometric information of tongue, speech and signature. The results showed that technique worked on real time environmental conditions.Correlation parameters were used for calculation and verifying the accuracy. In future we can apply new methods for steganography.

REFERENCES

[1] Cameron Whitelam, Nnamdi Osia and Thirismachos Bourlai, "Securing Multimodal Biometric Data through Watermarking and steganography," IEEE transactions on pattern analysis and machine intelligence, 2013.
[2] Vabhive B. Joshi, Mehal S. Raval, Suman Mitra, Priti P. Rage and S.K. Parulkar, "Reversible watermarking technique to enhance security of biometric authentication system,"Published in IEEE Conference on Multimedia and Expo, IEEE, Melbourne, pp. 1027-1032,2011.
[3] Emanuele Maiorana and Patrizio Campisi, "Fuzzy commitment for function based signature template protection," IEEE signal processing letters, vol. 17, no.3, 2010.
[4] Mandeep Kaur, Akshay Gidhar and Manvjeet Kaur, "Multimodal biometric system using speech and signature modalities," International Journal of Computer Applications, vol. 5, no.12, 2010.
[5] Nagesh Kumar and M.N. Shanmukha Swamy, "An efficient multimodal biometric face recognition using speech signal," 2010 IEEE.
[6] Seiichi Nakagawa, Longbiao Wang and Shinji Ohtusaka, "Speaker identification and verification of combining MFCC and phase information," IEEE transaction on audio, speech and language processing, vol.20, no.4, 2012.
[7] Dapinder Kaur, Gaganpreet Kaur and Dheerendra Singh, "Efficient and robust multimodal biometric system for feature level fusion (speech and signature)," International Journal of Computer Application, volume 75, no.5, 2013.
[8] Eshwarappa M.N. and Dr. Mrityunjaya V. Latte, "Multimodal biometric user authentication using speech, signature and handwriting features," International Journal of Advanced Computer Science and Applications, Special Issue on Artificial Intelligence, 2010.
[9] Niall A. Fox, Ralph Gross, Jeffery H. Cohn and Richard B. Rielly, "Robust biometric user identifications using automatic classifier fusion of speech, mouth and face experts," IEEE transaction on multimedia, vol. 9, no.4, 2007.
[10] P.B. Kathe and V.D. Dabhade, "Automated writer recognizer for offline text using scale invariant feature transformation descriptor," International Journal of Computer Applications Innovations and Trends in Computer and Communication Engineering (ITCCE-2014).
[11] Nikhil Nigam and Yogendra Kumar Jain, "Encoded hybrid DWT based watermarking scheme based onsingular matrix decomposition",

International Journal of Computer Applications, vol. 110, no. 14, 2015.
[12] Gaganpreet Kaur, Dr. Dheerendra Singh, "A Novel Biometric System based on Hybrid Fusion Speech, Signature and Tongue," International Journal of Computer Application, vol. 119,no. 7,pp. 30-39, 2015.
[13] Ross, A., and Jain, A., "Information Fusion in Biometrics", Pattern Recognition Letters, vol. 24, no. 13, pp. 2115-2125, 2003.
[14] Delac, K., and Grgic, M., "A Survey of Biometric Recognition Methods", in 46th International Symposium Electronics in Marine, ELMAR-2004, pp. 184-193,2004.
[15] Jain, A.K., Ross, A., and Prabhakar, S., "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 1782-1793, 2004.

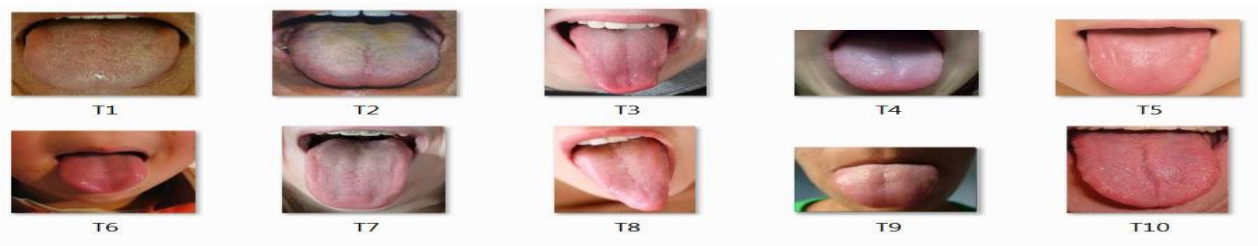
TABLE 1

CALCULATED RESULTS

S No.	Signature Samples	Tongue Samples	Speech Samples	Calculated Feature Values of Signature	Calculated Feature Values of Tongue	Calculated Feature Values of Speech	Result for identification
1	S1	T1	s1	STD=0.072 Mean=0.935 Variance=0.003 Entropy=0.340	STD=0.300 Mean=0.560 Variance=0.075 Entropy=0.790	PITCH=351.3 TEMPO=181.8 PULSE CLARITY=-0.016 ZERO CROSS=873.3 ROLL OFF=7332.4 CENTROID=3627.7 SPREAD=9.85	User 1 Identified
		T 2	s2	-	-	-	Wrong Match
		T3	s3	-	-	-	Wrong Match
2	S2	T1	s1	-	-	-	Wrong Match
		T2	s2	STD=0.054 Mean=0.946 Variance=0.004 Entropy=0.245	STD=0.190 Mean=0.231 Variance=0.037 Entropy=0.765	PITCH=351.6 TEMPO=153.9 PULSE CLARITY=-0.005 ZERO CROSS=913.1 ROLL OFF=7561.2 CD=3581.0 SPREAD=10.11	User 2 Identified
		T3	s3	-	-	-	Wrong Match

TABLE 2. TEST IMAGES USED[13]

a) Tongue Database



b) Signature Database [SVC 20]

c) Speech Database [CMU_ARCTIC]