Embedding of Iris Pattern to Ear and Face Images By using Watermarking Technology

Shivani Pandey[1] Sandeep Patil[2]
[2]Sr. Associate Professor
[1,2]Department of Electronics & Telecommunication Engineering
[1,2]Shri Shankaracharya Technical Campus Junwani, Bhilai, Chhattisgarh, India

Abstract- the Biometric template offers a dependable approach to the trouble of user authentication in identity management structures. Various biometric technologies were developed and effectively deployed around the arena which includes fingerprints, face, iris, palm-print, hand geometry, and signature. This method include the tree biometric trait such as iris, era and face for the biometric template security. Most biometric organizations which are presently in use, generally use a solitary biometric quality i.e. fingerprints because of its uniqueness and persistence, such system to set up identity, called uni-modal biometric structures that have a few obstacles. This work proposes a multimodal biometric scheme for identification purpose. Apart from that Biometric is the programmed recognition of entities based on their behavioral and biological representative. This work include biometric security which is the privacy issues derived from misuses of the template data. This proposed work include, the discrete wavelet transform ratio (DWT) and watermarking for security and to improve the template protection, especially for handling the misuse of security. So this work anticipated the biometric technique considers numerous traits such as Iris, Ear and Face for proposing the discriminative of liveliness. The recommended technique for Embedding of Iris data to Ear and Face Images Using DWT and Watermarking to improve Template Protection in Biometric Recognition is based on the following steps: (1) Embedding an Iris pattern to Ear and Face Images by Watermarking. (2) Matching is done by query images which is authenticated. The implementation is done by using MATLAB and the performance of the technique is analyzed with various performance parameters.

IndexTerms **– authentication, biometric, DWT, watermarking, embedding.**

I. INTRODUCTION

Currently a widespread assortment of presentations consist of trustworthy certification orders to endorse the personality of a person. Illustrations of such presentations take account of provided that admittance to constructions, mainframes, automated teller machine, cellular phones, bank financial statement etc. At the moment, our characteristics are corroborated more or less totally by one of two procedures - possessions that you bring with you and the possessions that you recall. Driver's excesses, passes and tokens are illustrations of the anterior, passwords and PINs are prototypes of the latter. But physical or carnal documents is informal to false. Most of the safekeeping systems uses passwords and peculiar proof of identity numbers for computer interpretations, bank ATM, email interpretations, and web sites. Tokens, identity card, passes, passports etc. can be absent, lifted or replicated. Passwords and PINs are without problems broken by hackers and can be predicted, disremembered, communal, or detected. So we have need of a modification in the approach we are acknowledged. Biometrics could be that amendment. They are an essential alteration in the way we are acknowledged. Nothing like old-fashioned documentation which you need either think of or bring with you, and in this manner the biometrics is you only.

The biometric is a biological and interactive representative of a humanoid being that can separate one somebody from a new. Fingerprints, ear, teeth, face, voice, iris patterns, hand vein, step or posture examination, and so on are round about case in point. Such individualities are matchless to an individual and habitually, though not permanently, extraordinarily challenging to fake. However, credentials ways and means based on a solo biometric type or algorithm may not make available acceptable credentials enactment and can be lay open to outbreaks. As well not one and all may be capable to use a different biometric. Perhaps, some individuals don't have worthy ridge in their fingerprints to be capable to practice in fingerprint corroboration coordination. So by means of various biometric modalities, can accomplish not simply developed safekeeping, but also a proof of identity coordination that can be used by more individuals.

The Unimodal biometric systems have definite restrictions approximating deafening data, non-universality, inter-class correspondences, intra-class discrepancy and spoofing. To overcome the technical hitches in unimodal biometrics and to growth the acknowledgment rate and the level of safekeeping, multimodal biometrics is used. A multimodal biometrics uses a mish mash of two or more biometric behaviors for authenticating the characteristics of somebody. Improved biometric characters used should be unassociated and the behaviors can be shared at altered levels as described below:

(a) Sensor level: The data from several sensors are joined to produce a new data from which features can be extracted in a sensor level of the biometric characteristics.

(b) Feature level: In this level of biometric characteristic the features acquired from altered traits are combined into a single one.

(c) Matching score level: The scores from different traits are incorporated to form a combined matching score in the matching score level of the biometric characteristics.

(d) Decision level: Each and every trait is pre-classified unconventionally. Final grouping is based on fusion of outputs of altered modalities in the decision level of the biometric characteristics.

This paper represent a multimodal biometric coordination to approve a person identity, in which we are using three trait such as iris, ear and face for improving template protection in biometric authentication system. This paper is systematized as follows: Section II describes the related work. Section III presents the proposed methodology of this work. Section IV proposes the results and analysis of this work, and finally last Section V includes the related conclusion and future scope of this work.

II. RELATED WORK

N. Lalithamani, and Dr.M. Sabrigiriraj addressed embedding of the iris data into hand vein images by using watermarking process and, showing a use of watermarking for encryption process by using a various algorithm. This paper proposed the steps including pre-processing, various template extraction, embedded image and stored it. After that, the accuracy, FAR and FRR ratio obtained by sum and product rule for different threshold value. [1]

Bismita Choudhury et al. proposed a cancelable biometric scheme using the concept of steganography. The proposed method used the combination of Huffman Encoding and Discrete Cosine Transformation (DCT) was taken as a non-invertible transformation. The transformed template was generated by embedding the Huffman Encoded bit stream of a randomly selected image in the DCT coefficients of the unwrapped iris image. The feature extraction is done by considering three types of features, Haar wavelet, Principal Component Analysis (PCA) and Gray Level Co-occurrence Matrix (GLCM). [2]

Lendale Venkateswarlu et al. proposed a transform which was based on double watermarking performance. The work included Arnold Transform (AT), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) and enhanced vigorous double watermarking performance with semi – fragility (RDWTSF) for medical metaphors. The medical image was scrambled by applying Arnold transform, individually DWT and DCT transformations with different repetitions values and inverse techniques of DWT and DCT. The double watermarking technique was simulated with several attacks using MATLAB. The host image double watermarked for getting high robustness and two different type of watermark was used were semi-fragile and robust. [3]

Sondes Ajili et al. proposed a combining SVD and DWT representation for participating data in medical images. The very first point comprised of addition an elusive watermark into the inventive medical image and verified the integrity of the medical image and the AES algorithm was used. This robustness was accomplished the serial turbo-code to increase the security of the watermark message against attacks, the hash function SHA-1, the Discrete Wavelet Transform space and the Singular Value Decomposition to expand the watermark veracity. [4]

Kaushik Deb et al. combined DWT and DCT constructed watermarking performance with small frequency watermarking with subjective correction has been proposed. The work proposed watermark was essentially injected into the low frequency of each DCT block of the designated coefficient set of DWT dominion. To increase the inaudibility, the watermark image was adjusted by the weighted correction in the spatial domain. [5]

U.S.N. Raju et al. proposed a hybrid watermarking performance which combines DCT and DWT and produced the watermarked image. The proposed method satisfies the requirement of watermarking practice which was robust. Here compared the MSE and PSNR values of the host image and the watermarked image and the proposed method improved the perceptibility of the watermarked image, by applying different scaling factors and after that, the BCR values for altered attacks are found worthy. [6]

Yagiz Sutcu ET al.2013, introduced a user-specific biometric information measure and evaluated measures using iris biometric. Here explored the assumption of the biometric example superiority on the biometric figures measurements and used different separations of the iris data with dissimilar quality levels. After that investigated the conclusion of encoding phase in the iris appreciation by using PCA and comparing results obtained from image and binary feature domain. [7]

III. PROPOSED METHODOLOGY

This chapter follows the proposed methodology of embedding iris data to ear and face images using watermarking with DWT-SVD techniques. The intention of our biometric acknowledgement system is to develop the template protection by embedding the iris data to ear and face images based on watermarking technology. The proposed technique of embedding of iris data to ear and face images using watermarking technology comprises embedding of iris pattern to ear and face images and after that the matching process is done with the ear image.

The proposed methodology of this work basically include the embedding of the iris pattern to ear and face images one by one by using watermarking in which the watermark extraction is also done. The given flow chart shows the overall embedding process which is done in this work. In the recognition phase an image pattern is extracted from embedded image and after that the matching is done with query image. In the result section of this methodology evaluated the various performance parameters including MSE, PSNR, BER, MAD, FAR and FRR.

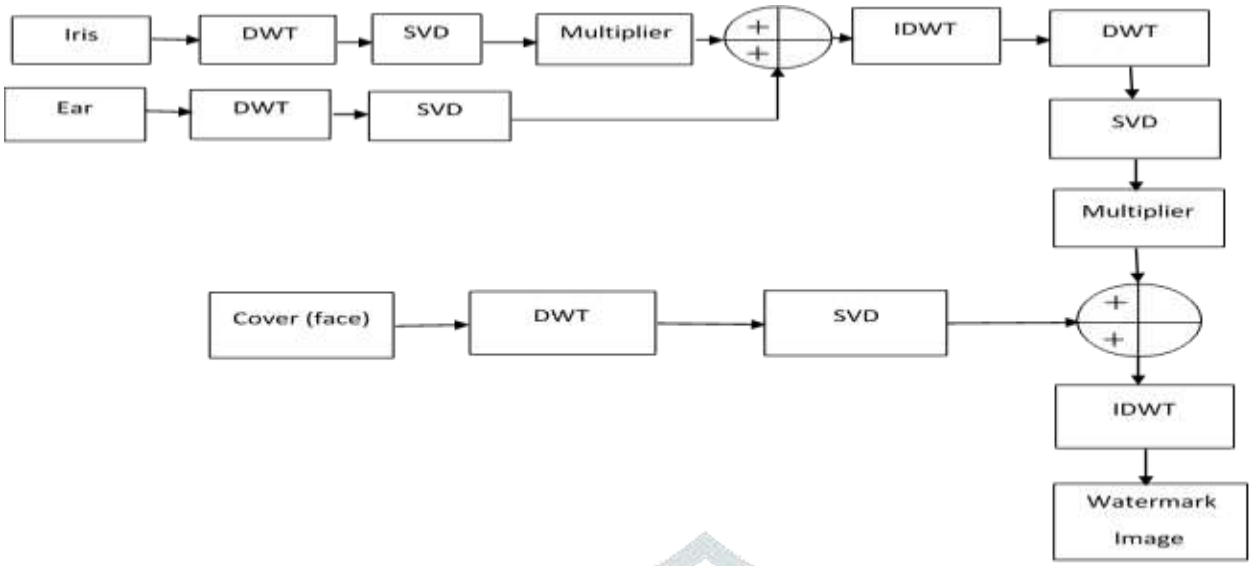

Figure 1: Block Diagram of the proposed methodology of Embedding

3.1 Analysis of DWT-SVD algorithm: The Discrete Wavelet Transform (DWT) is a manner for the transformation of a given purpose to the frequency domain. Spread over DWT to a digital image resembles to handing out the image by 2-D filters for each dimension. By cascading multiple filters and down sampling, the filters boundary the input image into four non-overlapping multiresolution sub-bands which are LL1, LH1, HL1, and HH1. The sub-band LL1 symbolizes the coarse-scale DWT coefficients while the sub-bands LH1, HL1, and HH1 symbolize the fine-scale of DWT coefficients. It is to reminder that when consuming multi-level DWT, the choice of element to be composed is left to the user; in the proposed algorithm, second and third level DWT was applied on the approximation components (LL) in each subsequent decomposition. But the possibility is presented to use in the least of the supplementary bands, such as decaying (LH). In wide-ranging, most of the image dynamism is determined at the lower frequency sub-bands LLx, and for that reason embedding watermarks in these sub-bands may cut down or degrade the image suggestively. Embedding in the low frequency sub-bands, nevertheless, could intensification robustness suggestively. On the other hand, the high frequency sub-bands HHx take account of the edges and textures of the image and the anthropoid eye is not by and large penetrating to alterations in such sub-bands. This allows the watermark to be embedded shorn of or without being perceived. Finding the middle ground implemented by many DWT-based watermarking algorithm, is to embed the watermark in the middle frequency sub-bands LHx and HLx where tolerable concert of noiselessness and robustness could be completed.

The Singular Value Decomposition (SVD) is a factorization of a real or compound matrix. It has many useful submissions in signal processing and statistics. The transform conditions that, for any specified m x n matrix a, there be present a factorization of the form: here, U is an m x n unitary matrix, D is an m x n diagonal matrix with nonnegative real numbers on the diagonal, and V is an n×n unitary matrix. The fundamentals of matrix D are called the singular values (SVs) of matrix A and are meticulously associated to the eigenvalues of the matrix A. The foremost draw of this matrix decomposition for digital watermarking is that a watermark can be injected using the singular value matrix D to assistance from the fact that the SVs are very stable as contrary to small fluctuations to the matrix A, contribution robustness to the watermark embedded within from external attacks that try to adapt the watermark without disturbing the host image. In accumulation, the non-negative Real SVs are sorted in descending order from d (1, 1), the topmost left portion in the diagonal of D towards d (m, n).

3.2 Embedding and Watermark Extraction: In the very first stage of encryption 1 performance, take an iris image as the message image 1 and the ear image as a cover image 1. Here the aim is to encrypt or hide the message image in the cover image by using the DWT-SVD algorithm with the 10% addition by using the 0.1 multiplier.

The arrangement for a short-lived explanation of the two transforms used in the proposed algorithm to watermark images. The two transforms are the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The two transform are applied in cascade in such a way to adventure their striking belongings.

When the DWT-SVD is performed and first encryption is done, then the 0.1 multiplier and summation is use here. The Multiplier block indicated as an integrated circuit multiplier. It can use the Multiplier block to appliance a number of supplementary functions, as well as multiplication. The examples take account of division, squares, and square roots. For example circuits, consult manufacturer datasheets etc., and by the summation, the sums of the series is perform here. After that the IDWT is perform which is stands for the Inverse discrete wavelet transform. The IDWT of input reconstruct signals from sub-bands with smaller bandwidths and slower sample rates and find the output of encryption 1 which is a watermarked ear image.

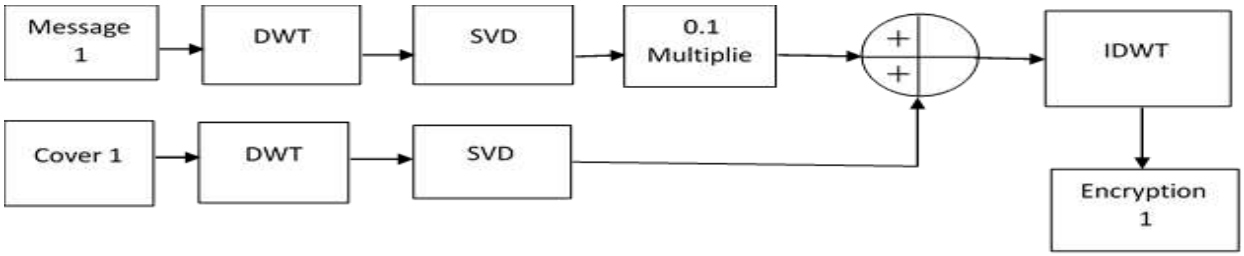

Figure 2: Block Diagram of the first Encryption

For the decryption1, we take the image of encryption 1 output as the first input and the same cover image1 (ear image) as the second input. Again apply the four levels of DWT and SVD algorithm for watermarking. Here the 10% subtraction is used and after that the IDWT is performed. In the result of the decryption1, messege1 is the output.

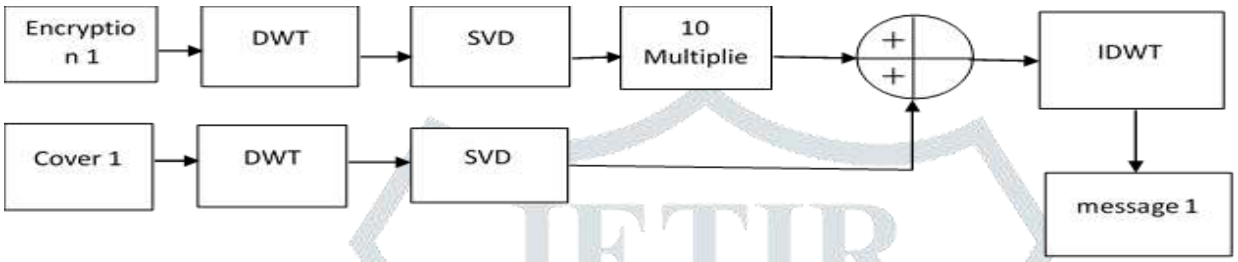

Figure 3: Block Diagram of first Decryption

Now encryption 2 is performing and for this taken the message 2 (ear) as the first input of encryption2 and cover image2 which is the face image is taken as the second input of encryption2. After that here perform the DWT-SVD separately for both the inputs and take the 0.1 multiplier and the summation. When the sum is performed then IDWT is done and in the output will get an encryption2 result which is an encrypt face image in which the encrypt ear image is hide.

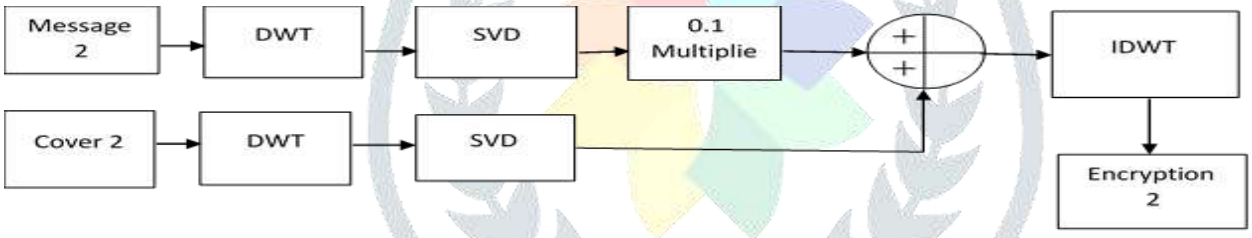

Figure 4: Block Diagram of second Encryption

For the decryption2, taken the encryption 2 output as the first input of decryption2 and the same cover image2 as the second input. Now, again perform DWT-SVD separately and here also the 10% subtraction is done. After that the IDWT is perform and getting the final output of embedding which is actually the encryption1 output is decrypt in the ear as well as iris image.

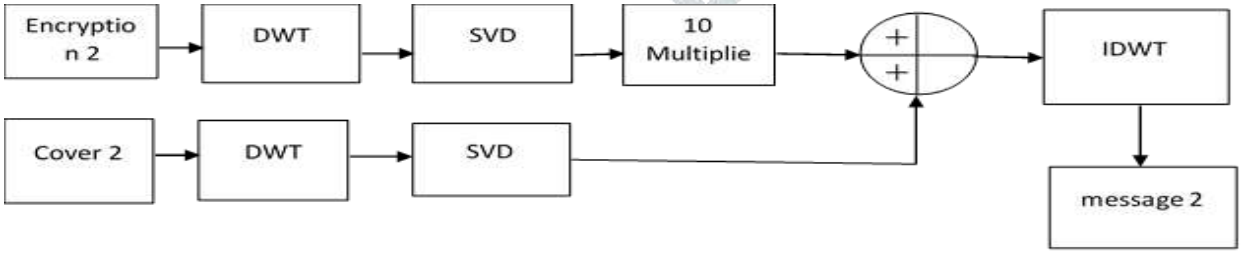

Figure 5: Block Diagram of second Decryption

When the whole embedding process is done then concluded that the decrypt image quality is not as good as the original sample images. In this proposed work, the whole process is done with the RGB (Red, Green, and Blue) image which give the very good quality.

3.3 Matching: Now in the recognition phase after the watermark extraction and embedding the matching is done with the query image. Here the mish mash of linear and exponential function is used for matching. The value of weight is assigned linearly if the value of matching score is less than the threshold; otherwise exponential weightage is given to the score. So if matching score is greater than threshold value then individual is allowed to enter the system otherwise rejected or if the matching score is less than

10; as taken the threshold value from 1 to 10, then the source is authenticated, otherwise it shows the source is unknown. Depend on the different threshold value, the FAR and FRR ratio is evaluated here.

IV. EXPERIMENT RESULT

The proposed method had implemented by using MATLAB 2014 version in a system having 4 GB RAM and 2.6 GHz AMD processor, Minimum 15 GB HDD Space for MATLAB. In this method take a high quality color images of iris, ear and face for use in research and evaluation. The pixel resolution of the collected iris image is 1200 x 1146, pixel resolution of collected ear image is 492 x 702 and the pixel resolution of face image is 375 x 450.

MSE: MSE is a mean squared normalized error performance function which is a network performance function. It measures the network's performance according to the mean of squared errors. The above equation shows the Mean Square Error between the images I which is the original image and I' which is taken as the watermarked image and both image with the size mxn.

$$\mathbf{MSE} = \frac{1}{MN\sum_{x=1}^{M}\sum_{x=1}^{N}(I(x,y)I'(x,y))^2}$$

PSNR: PSNR is stand for the Peak Signal-to-Noise Ratio. Peak signal-to-noise ratio is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. The visual quality of the proposed work with the watermarking impact is measured using the Peak Signal to Noise Ratio (PSNR). The formula foe PSNR is shown below:

$$\mathbf{PSNR} = \mathbf{10}\log_{10}\left(\frac{255^2}{MSE}\right)$$

BER: Bit Error Rate is a function of the energy per bit to noise power spectral density ratio (Eb/N0) often abbreviated as BER. Basically the BER is the number of bit errors divided by the total number of transferred bits during a studied time interval. Bit error ratio is a unit less performance measurements. The BER of the extracted watermark, compared with the original image by the formula:

$$\mathbf{BER} = \frac{PSNR}{8}$$

MAD: In statistics, the median absolute deviation (MAD) is a robust measure of the variability of a univariate sample of quantitative data. It can also refer to the population parameter that is estimated by the MAD calculated from a sample. For a univariate data set X1, X2…Xn, the MAD is defined as the median of the absolute deviations from the data's median:

$$\mathbf{MAD = median\ (|Xi - median(X)|)}$$

FAR: The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

$$\mathbf{FAR} = \frac{GMS}{NGRA}$$

FRR: The false recognition rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR typically is stated as the ratio of the number of false recognitions divided by the number of identification attempts.

$$\mathbf{FRR} = \frac{IMS}{NIRA}$$

The Table shows the evaluated performance parameters obtained from Embedding:

S No.	Dimension	MSE	PSNR	BER	MAD	FAR	FRR
1.	275×183	27.2698	77.7675	9.72093	81.8095	0.912665	0.0873353
2.	300×183	28.1623	77.4454	9.68068	84.4869	0.917297	0.0827031
3.	220×183	26.764	77.9547	9.74434	80.292	0.932042	0.0679584
4.	224×183	25.0429	78.6194	9.82742	75.1288	0.945178	0.0548218
5.	239×183	25.541	78.4224	9.8028	76.623	0.918321	0.0816795

6.	300×183	27.9551	77.5193	9.68991	83.8654	0.913306	0.0866941
7.	290×183	34.2336	75.4932	9.43665	102.701	0.904628	0.0953721
8.	260×183	26.8448	77.9245	9.74054	80.5345	0.931379	0.686212
9.	1200×1146	23.8502	79.1073	9.88842	71.5507	0.930875	0.0691254

Table 1: Evaluation Parameters for Different Iris Sample

The above table, shows the value of different performance parameter which is evaluated from taking the different Iris pattern and with the same cover images, calculated by using the algorithm DWT-SVD. The values shows that the Iris image which is taken in this proposed work is more suitable as compare to other iris pattern and have a good embedding strength. So in this propose work the result is much improved as represent here.

V. CONCLUSION

In this work, have presented a well-organized biometric recognition arrangement for template protection. The main issues with the biometric template protection was the uni-modality of it. So, this proposed work included the three types of biometric modalities and the project is done with multimodal biometric traits. In the proposed work, used a watermarking technology to improve the template protection based on the three modalities the iris, ear and the face. This work have done in RGB which represent a good approach of work. In the very first stage of embedding in this method take two sample images (iris and ear) and a cover image (face) which were the color image with very good quality. After that the iris image is watermarked in the ear image by the encryption, then the encrypted ear image is again encrypt in the face image. This two stage of encryption give effective result for watermarking. In the decryption process, the encrypt ear image was decrypt from face image and, secondly the iris image is also decrypted from ear image. This was the process of two stage decryption. The three biometric modalities and two stage of encryption as well as decryption were a very effective idea for the presented work and it give good security in case of biometric template protection and watermarking.

As a final point the extracted features were matched with input query image which is ear image and the matching is done. The matching process in this particular embedding work, was an advance effort for the experiment. If the input query image was ear only then the source get authenticated otherwise the experiment shown an unknown source. The algorithm used here was a very effective and suitable DWT-SVD algorithm which given very good result for the whole project. The results obtained from the experimentation shows that the proposed watermarking techniques provide better results with higher accuracy.

ACKNOWLEDGEMENT

This work is product of four semester of learning and dialogues with my project supervisor **Mr. Sandeep Patil**. I sincerely thanks him for his numerous suggestions and commend his patience. It was an honor to have him as my project supervisor. I also want to express my gratitude towards my family member for their encouragement and support.

REFERENCES

[1] N. Lalithamani, Dr.M. Sabrigiriraj, 2015, 'Embedding of Iris Data to Hand Vein Image Using Watermarking Technology to Improve Template Protection in biometric recognition' IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT): 1-7

[2] Bismita Choudhury, Patrick Then, Valliappan Raman, Biju Issac, Manas Kumar Haldar, 2016, 'Cancelable Iris Biometrics Based on Data Hiding Schemes' IEEE Student Conference on Research and Development (SCOReD) :1-6

[3] Lendale Venkateswarlu, N Vyaghreswara Rao, B Eswara Reddy, 2017, 'A Robust Double Watermarking Technique for Medical Images with Semi-Fragility' IEEE International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT): 126-131

[4] Sondes Ajili, Mohamed Ali Hajjaji, Abdellatif Mtibaa, 2015, 'Hybrid SVD- DWT watermarking technique using AES algorithm for medical image safe transfer' IEEE international conference on Sciences and Techniques of Automatic control & computer engineering – STA: 69-74

[5] Kaushik Deb, Md. Sajib Al-Seraj, Md. Moshiul Hoque, Md. Iqbal Hasan Sarkar, 2012, 'Combined DWT-DCT Based Digital Image Watermarking Technique for Copyright Protection' IEEE 7th International Conference on Electrical and Computer Engineering: 458-461

[6] U.S.N. Raju, Kamalakanta Sethi, Sunaina Choudhary, Priyanka Jain, 2015, 'A New Hybrid Watermarking Technique using DCT and DWT based on Scaling Factor' IEEE 1st International conference on futuristic trend in computational analysis and knowledge management (ABLAZE): 232-235

[7] Yagiz Sutcu, Elham Tabassi, Husrev T. Sencar, Nasir Memon, 2013, 'What is Biometric Information and How to Measure It?' IEEE International Conference on Technologies for Homeland Security (HST): 67 - 72

[8] Jinjin Dong, Xiao Meng, Meng Chen, ZhifangWang, 2017, 'Template Protection Based on DNA Coding For multimodal biometric recognition' IEEE 4th International Conference on Systems and Informatics (ICSAI): 1738-1742

[9] Fathima N, Smitha Satheesh, 2017, 'Multi-Modal Biometric Security with Multi- Algorithm' IEEE International Conference on Trends in Electronics and Informatics ICEI: 440-443

[10] Bingchen H. Guo, Mark S. Nixon, John N. Carter, 2018, 'Fusion Analysis of Soft Biometrics for Recognition at a Distance' IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA): 1 - 8

[11] Keshav Gupta, 2017, 'Advances in Multi Modal Biometric Systems: A Brief Review' IEEE International Conference on Computing, Communication and Automation (ICCCA): 262-267

[12] Puneet Gupta, Phalguni Gupta, 2018, 'Multi-biometric Authentication System using Slap Fingerprints, Palm Dorsal Vein and Hand Geometry' IEEE Transactions on Industrial Electronics: 1 - 1

[13] Cheniti Mohamed, Zahid Akhtar, Boukezzoula Naceur Eddine,Tiago H. Falk, 2017, 'Combining Left and Right Wrist Vein Images for Personal Verification' IEEE Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA): 1 - 6

[14] Karthikeyan Shanmugasundaram, Ahmad Sufril Azlan Mohamed, Nur Intan Raihana Ruhaiyem, 2017, 'An Overview of Hand-based Multimodal Biometric System using Multi-Classifier Score Fusion with Score Normalization' IEEE International Conference on Signal Processing and Communication (ICSPC): 53-57

[15] Ankur Shukla, Shishir Kumar, 2016, 'Analysis of Secure Watermarking Based on DWT-SVD Technique for Piracy' IEEE International Conference on Computing, Communication and Automation (ICCCA): 1110-1115