ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Embedding of Iris To Hand Vein Images Based on Watermarking Technology for Biometric Recognition

K.S.Chamini
PG Scholar,
Department of ECE,
Sri Venkatesa Perumal College of Engineering and Technology,
Puttur.

C. Manikanta, M.Tech
Assistant Professor,
Department of ECE,
Sri Venkatesa Perumal College of Engineering and Technology,
Puttur.

ABSTRACT

Biometric recognition is noteworthy method for recognition of person in recent years. Here, a common concern is biometric security which is the privacy issues derived fromstorage and misuses of the template data. In order to handle this issue, researches have proposed different algorithms to be confronted by security of biometric systems. Two major ways are, (1) Encryption, and (2) watermarking by securing biometric images and templates. In this paper, we utilize a watermarking technology to improve the template security in biometric authentication. According to, two modalities such as, iris and hand vein is taken to preserve the characteristics of liveliness and permanency. Our proposed technique for embedding of iris data to hand vein images using watermarking technology to improve template protection in biometric recognition is done based on the following steps, i) pre-processing of iris and hand vein images, ii)iris template extraction, iii) Vein extraction, iv) Embedding of iris pattern to vein images based on region of interest, v) Storing embedded images. In the recognition phase, iris pattern is extracted from the embedded image and then, matching is done with query images. The final decision of authentication is done based on the product rule-based score level fusion. The implementation is done using MATLAB and the performance of the technique is analyzed with FAR, FRR and accuracy.

Keywords-watermarking; embedding; extraction; authentication.

1. INTRODUCTION

Classical watermarking introduces permanent distortions; reversible watermarking not only extracts the embedded data, but also recovers the original host signal/image without any distortion. So far, three major approaches have already been developed for image reversible watermarking. They are reversible watermarking based on lossless compression, on histogram shifting and on difference expansion.

The lossless compression based approach substitutes a part of the host with the compressed code of the substituted part and the watermark etc. In order to avoid artifacts, the substitution should be applied on the least significant bits area where the compression ratio is poor. This limits the efficiency of the lossless compression reversible watermarking approach.

A more efficient solution is the histogram shifting approach. The histogram of a pixel based image feature (gray level, pixel difference, prediction error, interpolation error) is considered. A histogram bin is selected and the space for data embedding is created into an adjacent bin (either the bin located at the left or at the right). For instance, let p be the value of the selected bin and letp+1 (the bin to its right) be considered for data embedding. The features greater than pare shifted with one position (by modifying with one gray level the value of the corresponding pixels). Furthermore, the embedding is performed into the pixels with the feature value equal to p. When a zero is embedded the pixel is left unchanged, otherwise it is modified with one gray level in order to change the feature from p to p+1.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The procedure is similar if p−1 is considered for embedding, except that the shifting proceeds to the left. In a single embedding level, the approach provides an embedding capacity of the same order as the size of the selected bin. For this reason, the simple gray level histogram used in the original approach was replaced by Laplacian distributed histograms, with a prominent maximum bin, like the prediction error histogram and so on. The original approach considered the embedding into the maximum of the histogram in order to maximize the embedding bit-rate. Several other strategies have also been investigated. For instance, the simultaneous embedding into the maximum and the second in rank doubles the embedding bit-rate provided in a single embedding level .For embedding less than the size of the two largest histogram bins,a very efficient histogram shifting was proposed. The embedding is performed into the smallest two bins, one from the left and the other for the right, that provide the needed capacity. Since only the tails of the histogram must be shifted, the distortion is minimized. As the required embedding capacity increases, more embedding stages are performed. While in a single embedding stage the histogram shifting approach introduces distortion of at most one graylevel per pixel, this is no longer true for multiple embedding levels. In such cases, the most efficient approach is difference expansion (DE).

II. CONVENTIONAL METHODS

In the image-processing applications, the conventional methods that are most frequently used are cryptography, watermarking and steganography using Least- Significant Bit (LSB) Algorithm. Cryptography is the method in which encryption and decryption are performed based on the secret key, which is known only to the sender and receiver. The original information is embedded by following some encoding process in which the data is re-inserted based on certain procedure. In order to decode the message at the receiver, the reverse process is followed which is done at the encoding process. The difference between steganography and cryptography is that

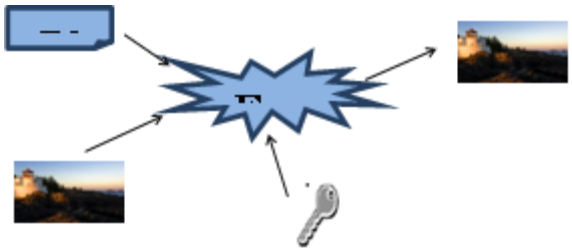

Fig.1 (a). Encryption Process

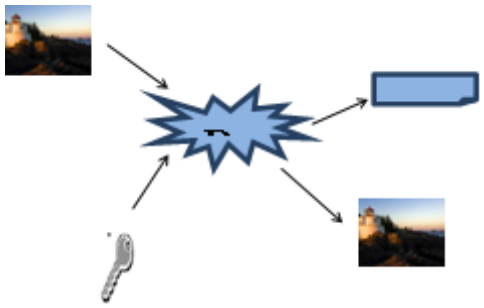

Fig.1 (b). Decryption Process

Cryptography is preferred to keep the contents of the messagesecretly whereas steganography is the method which keeps the existence of the message secret. These two methods protect information from the unwanted parties and security attacks. The other technology that is closely related to these methods is digital water-marking, in which an image is embedded into the original image such that it helps in signifying the ownership for the purpose of copyright protection[5].

Water-marking technique enables the intellectual property of the owner to identify the customers who break their licensing agreement by supplying the property to third parties. Fig.2(a) and 2(b) represents the encryption and decryption processes in cryptography. This paper describes the steganography algorithm that is most suitable for business and in commercial applications.

III. IMAGE ENCRYPTION

The information security is used from old ages differentpersonusingdifferenttechniquetosecuretheirdata.Followingaresometechniquesthatusesforsecurityofimages from ancient age to till date

A. Steganography

B. Watermarking Technique

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

C.VisualCryptography

A) STEGANOGRAPHY

Thesteganographywordcomesfromthe Greekword Steganos,whichisusedtocoverorsecretandagrapy,isusedforwritingordrawing.Therefore,steganographyis,literally,coveredwriting.Themainideaforcoveringtheinformationorsteganographyisusedforsecurecommunicationinacompletelyundetectablemannerandtoavoiddrawingsuspiciontothetransmissionofahiddendata[4].Duringthetransmissionprocess,characteristicsofthesemethodsaretochangeinthestructureandfeaturessoasnottobeidentifiablebyhumaneye. Digitalvideos,images,soundfiles,andotherfilesofcomputerthatcontainperceptuallyimportantinformationcanbeusedas–coversorcarrierstohidesecretmessages.Afterembeddingamessageintothe cover-image,aso-called–segosimageisobtained.

In[2]Security,Capacityandrobustnessarethreedifferent aspectswhichisaffectingsteganographyanditsusefulness. Capacityisusedtotheamountofinformationthatcanbehiddeninthecovermedium.Securityrelatestoaneavesdropper' sinabilitytodetecthiddeninformationandrobustnessisthe amountofmodificationthesegomediumcanwithstandbefo reanadversarycandestroythehiddeninformation.

Theconceptofthemosaicimagesin[1]wascreatedperfectly andithasbeenwidelyused.Fourtypesofmosaicimagesnam elycrystallizationmosaic,ancientmosaic,photomosaican dpuzzleimagemosaicareproposedin[2].Inthefirsttwotyp es,thesourceimageissplitintotileimageandthenitisrecons tructedbypaintingthetilesandtheyarenamedastile images.Thenexttwotypesincludeobtaining targetimage andwiththehelpofdatabase,coverimagehasbeenobtained. Theymaybe calledasmulti-picturemosaics.

B)WATERMARKINGTECHNIQUE

Watermarkingisalsooneofthetechniqueusedtohidethedigitalimage,Digitalwatermarkingisaprocessofembedding (hiding)markswhicharetypicallyinvisibleandthatcanbeextractedonlybyowner'softheauthentication.Thisisthetechnologywhichisusedin[15]withthe imagethatcannotbemisusedbyanyotherunauthorizedmissusers.

Thistechnologyallowsanyonetodowithoutanydistortion andkeepingmuchbetterqualityofstegnoimage,alsoinasecuredandreliablemannerguaranteeingefficientandretrievalsofsecretfile.Digitalwatermarkingfindswideapplication insecurity,authentication,copyrightprotectionandallwalksofinternetapplications.Therehasbeeneffectivegrowthindevelopingtechniquestodiscouragetheunauthorizedduplicationofapplicationsanddata.Thewatermarkingtechnique isone,whichisfeasibleanddesigntoprotecttheapplicationsanddatarelated.Theterm'cover'isusedtodescribetheoriginalmessageinwhichitwillhideoursecretmessage,data fileorimagefile.Invisiblewatermarkingandvisiblewatermarkingarethetwoimportanttypesoftheabovesaidtechnology.

Themainobjectiveofthispackageistoreducetheunauthorizedduplicationofapplicationsanddata,providecopyrightprotections,security,andauthentication,toallwalksofinternetapplications.

C)VISUALCRYPTOGRAPHY

VisualCryptographyisusedtohideinformationinimages,a specialencryptiontechniqueinsuchawaythatencryptedimagecanbedecryptedbythehumaneyes,ifthecorrectkeyimageisused.ThetechniquewasproposedbyNaorandShamirin1994[1].Itisusestwotransparentimages.Oneimagecontainsimagecontainsthesecretinformationandtheotherrandompixels.Itisnotpossibletogetthesecretinformationfromanyoneoftheimages.Bothlayersandtransparentimagesarerequiredtogettheactualinformation.The easiestwaytoimplement Visual Cryptographyis toprintthetwolayersontoatransparentsheet.

VI. PROPOSED METHOD

The aim of our biometric recognition system is to improve the template protection by embedding the iris data to hand vein images based on watermarking technology. The proposed technique of embedding of iris data to hand vein images using watermarking technology consist of following steps, i) pre processing of iris and hand vein images, ii) iris template extraction, iii) Vein extraction, iv) Embedding of iris pattern to vein images based on region of interest, v) Storing embedded images.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

(i) Irish Image Pre-processing and key generation

The initial stage of our proposed method is pre-processing in which the iris images are acquired and process to extract the iris key. By subsequent localization, the information related with iris part is selected from the entire image.

a) Iris Localization

Nevertheless, localization can be said successful, when it is accomplished with minimum absences in the number of pixels inside the circle boundary. The reduction of number of pixels inside the circle boundary leads to fast and easy computation. Then, the peaks of the gradient image can be localized using non-maximum suppression. The process of non-maximum suppression on a pixel with its gradient imgrad(x,y) and orientation theta(x,y) can be framed by using an edge intersects through two of its eight neighborhood connected pixels. A point at (x,y) can be said as maximum in such a way that its pixel value should not be smaller than the pixel values of the two intersection points. Subsequently, hysteresis thresholding is performed so that the weak edges that are below certain threshold value and that are not connected with an edge, which is above high threshold, through a chain of pixels, which are above the low threshold, can be eliminated. Boundaries of the iris and the pupil are determined to perform edge detection process. These boundaries and radii can be determined by integro-differential operator proposed by Daugman.

The aforesaid operator searches the gradient image along with boundary of circles with high radii and hence it behaves as a circular edge detector. The circles centers and radii can be calculated using the maximum sum, which can be determined based on the likelihood of all circles.Few concerns are associated with Hough transformation. They are, determining threshold values by trial and error basis and intensification in computation. These issues can be resolved by using eight-way symmetric points in the circle for each search point and radius. Thresholding concept can be used to segregate eyelashes and these pixels are marked as noisy pixels, because they are not included in the iris key.

b) Image Normalization

The next stage after iris segmentation is normalization to generate iris key and their comparisons. Normalization process is comprised of two steps that are unwrapping the iris and conversion of it into polar equivalent. This can be done using Daugman's rubber sheet model. Center of the pixel is set as the reference point and the points are converted from Cartesian scale to polar scale using a remapping formula.

Radial resolution and angular resolution of the image are set to 100 and 2400, respectively. An equivalent position for each iris pixel is determined in the polar scale. "interp2" function is exploited to interpolate the normalized image to size of the original image. A normalized value can be obtained by dividing NaN, which is obtained through the parts in the normalized image, using the sum of the parts.

c) Encoding

Generation of iris key is defined as the final process for which the most unique feature in the iris pattern is extracted.

As the assigned phase angles are independent to the image contrast, only the phase information from the patter is used. Due the dependency of amplitude information with inappropriate factors, it is not used. According Daugman, phase information can be extracted using 2D Gabor wavelets. It estimates the quadrant in which the resulting phasor lies. This can be accomplished using the following equation (3).

After embedding all the bit of the iris template J(x,y) inhand vein image an IDWT (Inverse Discrete Wavelet Transform) is applied to the watermarked hand vein coefficient to generate the final secure watermarked hand vein image. the watermark embedding process is shown in the figure below,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

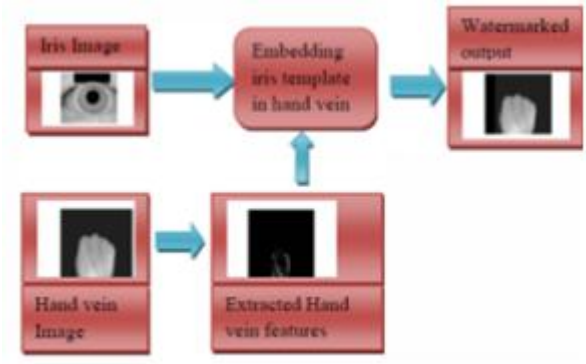

Fig.2:Water Mark embedding

Recognition Phase using Score level fusion

The recognition phase is divided in two major steps.

Step.I. Watermark extraction

In this recognition phase the watermarked image is given as input and the iris key and hand vein features are extracted. The watermark extraction phase consists of various steps.

The input is watermarked image Hw(x,y) and the size of watermarked image Hs(x,y)and the output is recovered watermark image Rw(x, y) .

I)The watermarked image is divided in to the detail sub band of watermarked image in to blocks. The each block of the watermarked image is of size 2M -1 x 2N -1.

2) Identify the value below the threshold T(x,y) in each blockwhich has the first coefficient with positive phase.

3) The pixel value 1 from the watermarked image is extracted if the embedded pixel value is greater than the mean pixelvalue otherwise pixel value '0' is extracted. This process is repeated until all the pixels from the watermarked image are y given in equation (12) below

$$Hs(x,y) = \{I, B(i) > Bn, \circ < i < n$$

$$0, Otherwise$$

4) A matrix equal to the size of watermark image Hw(x,y) and the extracted pixels are placed in it to obtain In recognition phase the both iris and vein image of an individual is taken. Then both the obtained iris image and the hand vein image are pre-processed separately as by the above procedures. After this pre-processing stage the iris key from the iris image and the vein features from the vein image are obtained. Further in order to find whether the input user is genuine or imposter we have to compare the obtained feature with the feature stored in the database. But in the database the iris key is embedded in the hand vein image to improve the template protection. So here we have to extract the iris key and vein image separately.

Step 2: Matching

Now the distance between iris key generated from the input query image and iris key extracted from the embedded image stored in database is determined. The matching distance for the input iris key and the extracted iris key from embedded image is denoted as Diris. Likewise the pre-processed vein image of the same person is matched with the vein image feature extracted from the embedded image stored in database. Finally a matching distance D:vem for the vein image is determined. Further the two normalized similarity distance Diris and DVein are fused linearly.

Where a andbare two weight values that can be determined using some function. In this paper a combination of linear and exponential function is used. 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. The value of MS is used as the matching score. So if matching score is greater than threshold value then individual is allowed to enter the system otherwise rejected.

V EXPERIMENTAL RESULTS

5.1 STARTING Mat alb

1. Start mat lab from start menu or windows shortcut icon
   Start->All Programs->Mat lab 13.2
2. Upon running Mat lab, a command window is appearing as shown in figure 5.1.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

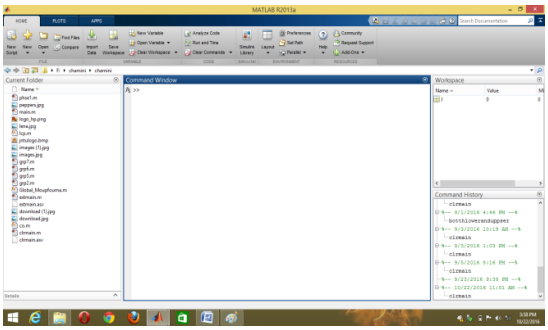

Fig 5.1 Command window

3 Go to open menu then select code and open as shown in figure 5.2

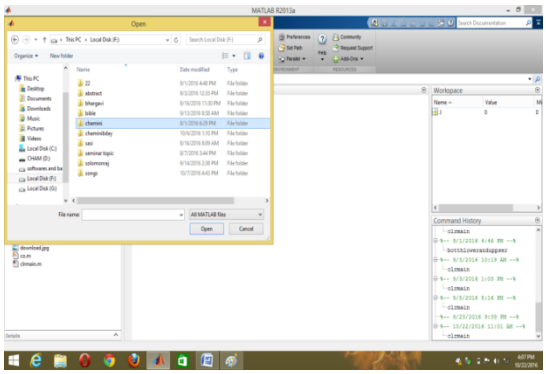

Fig 5.2 Opening code dialog box

4. Code is displaying as shown in figure 5.3

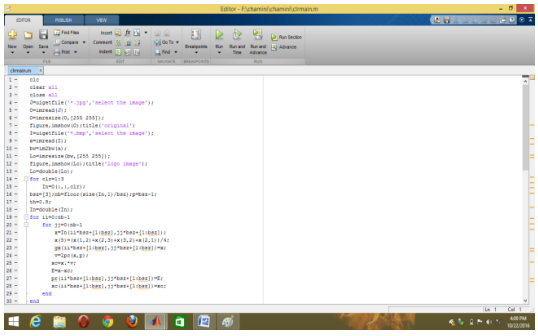

Fig 5.3 displaying code window

5. A select file to open dialog box is displayed to select any image and open as Shown in figure 5.4

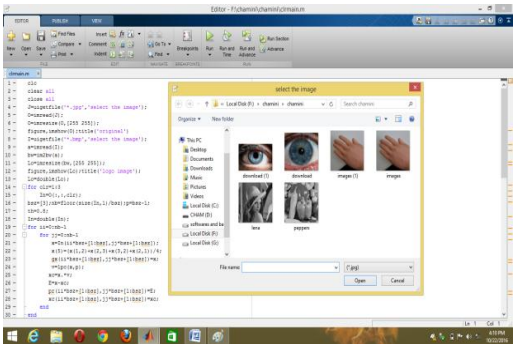

Fig 5.4 select file to open dialog box

6. The prediction error method results, ETC results are displayed as shown in figure 5.5

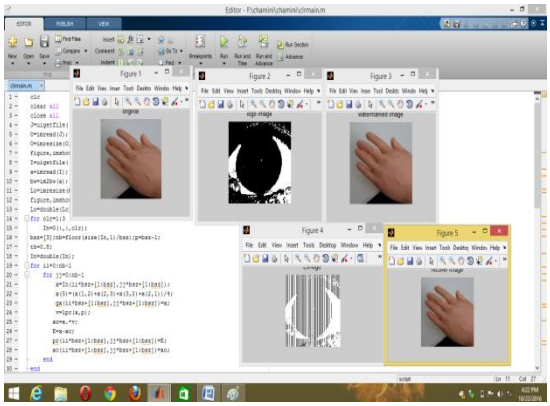

Fig 5.5 prediction error method results and ETC result

7. The PSNR, MSE, RMSE values will be displayed in command window as shown in figure 5.6

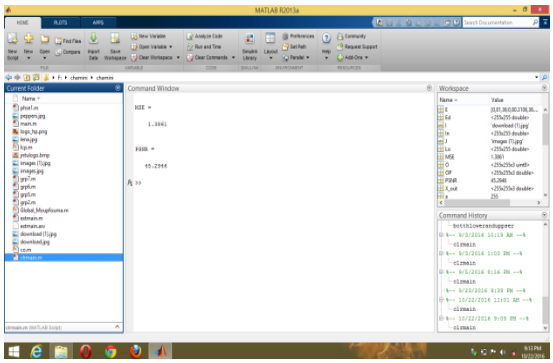

Fig 5.6 command window displaying PSNR, MSE values

PSNR: PSNR is most commonly used to measure the quality offer image compression. The signal in this case is the original data, and noise is the error introduced by compression. When comparing compression, PSNR is a human perception of reconstruction quality. The PSNR is calculated based on color texture based image segmentation. The PSNR range between [0.1], the higher is better. PSNR=20*log10(255/sqrt(MSE)).

PSNR: 45.2946

MSE: Mean square error (MSE) is calculated pixel by pixel by adding up the squared difference of the entire pixel and dividing by the total pixel count.

MSE: 1.3861

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

5.2 SIMULATION RESULTS

After running the program (according to the code) initially selects the image. so, the selected image will be original image and it is shown as in below figure 1

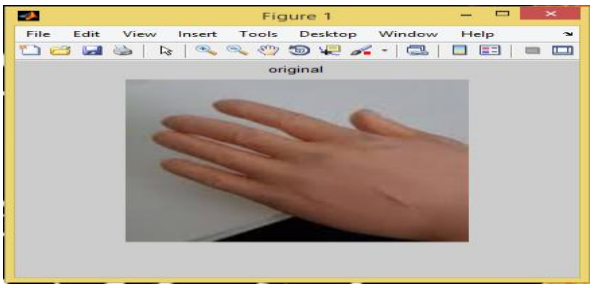

Fig 5.7 Original Image

After selecting the original image it again ask hands then select the embedding image as per as our base paper hand veins figure 2.

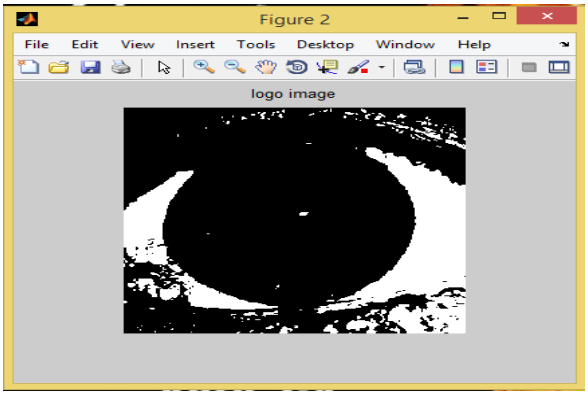

Fig 5.8 Logo Image

So, the combination of Iris and watermarked hand veins are shown in figure 3

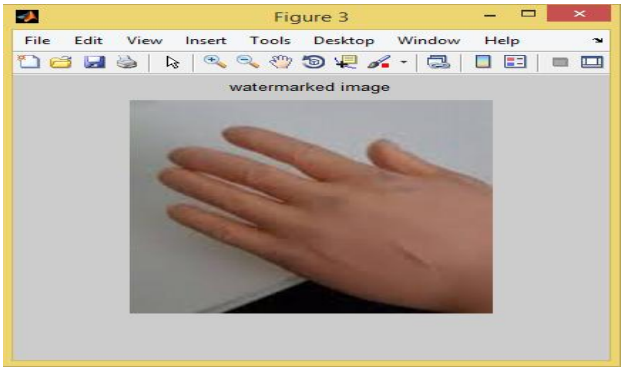

Fig 5.9 Watermarked Image

Extracting or recovering the data from watermarked image is required figure 4 and 5 the extracting images are

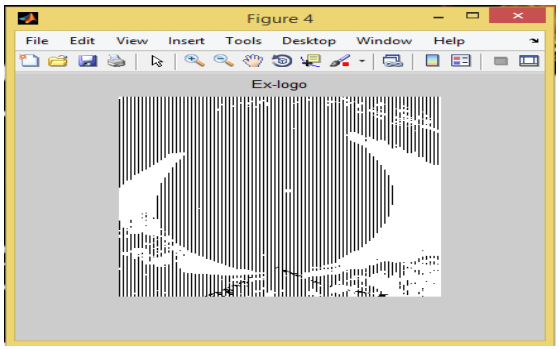

Fig 5.10 Ex-logo image

Fig 5.11 Recover Image

The experimental results have shown that the security of our proposed method s reasonably high. The reconstructed image quality is measured in terms of PSNR. The compressed image is measured in terms of Quality measures like MSE, PSNR.

The quality measured values of MSE is 1.3861,PSNR value is 45.2946.

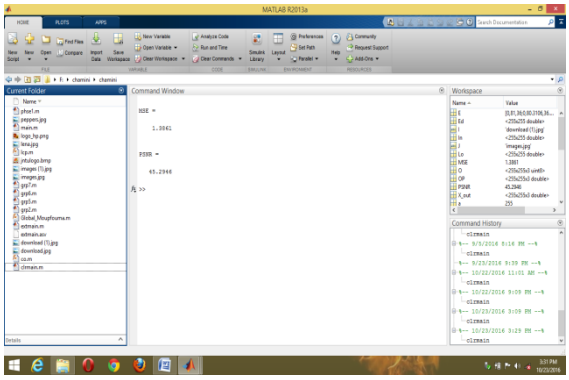

Fig 5.12 Output Values

CONCLUSION

Before going any further, it should be noticed that the proposed local prediction scheme applies regardless of the size or the shape of the prediction context. If the watermarking is done pixel by pixel in raster-scan

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

order, it appears that only half of the pixels within the block are original pixels.

The other half of pixels has already been modified by the watermarking procedure (see Fi In this paper, we have presented an efficient biometric recognition system for template protection. We have used a watermarking technology to improve the template protection based on the two modalities the iris and the hand vein. The iris template was extracted from the pre-processed iris image.

FUTURE SCOPE

Then the features of the hand vein were extracted. After this the extracted iris template was embedded in to the hand vein and stored in the database. Subsequently in recognition phase the iris template and hand vein features were extracted from the watermarked image. Finally the extracted features were matched with input query image. The final decision of authentication was done based on the product rule-based score level fusion.

The results obtained from the experimentation shows that our proposed watermarking techniques provide better results with higher accuracy. The accuracy of our proposed method can be further improved by improving the embedding strength and embedding location by various search algorithms.

References

[1] P. Poongodi, and P. Betty, "A Study on Biometric Template Protection Techniques," International Journal of Engineering Trends and Technology (IJETT), vol. 7, no. 4, 2014.

[2] R. Yadav, Kamaldeep, R. Saini, and R. Nandal, "Biometric Template security using Invisible Watermarking With Minimum Degradation in Quality of Template,International Journal on Computer Science and Engineering, vol. 3, no. 12, 20 I I.

[3] J.L. Jimenez, R.S. Reillo and B.F. Saavedra, "Iris Biometrics for EmbeddedSystems," IEEE Transactions on Very Large Scale Integration (VLSI) systems, vol. 19, no. 2,20 I I.

[4] P.S. Revenkar, A Anjum and W.Z. Gandhare,"Secure Iris Authentication UsingVisual Cryptography," International Journal of Computer Science and Information Security, vol. 7, noJ, 20 I O.

[5] AK. Jain, A Ross, and U. Uludag, "Biometric Template Security Challenges and Solutions," In Proceedings of European Signal Processing Conference, 2005.

[6] N. Hajare, A Borage, N. Kamble, and S. Shinde, "Biometric Template Security Using Visual Cryptography," Journal of Engineering Research and Applications (IJERA), vol. 3, no. 2, pp. I 320-1 323,2013.

[7] C.L. Li, Y.H. Wang, and B. Ma, "Protecting Biometric Templates using LBP-based Authentication Watermarking," Chinese Conference on Pattern Recognition, pp. I -5,2009.

[8] M. Arjunwadkar, and R.V. Kulkarni, "Robust Security Model for Biometric Template Protection using Chaos Phenomenon,"International Journal of Computer Applications, vol. 3, no. 6, 2010.

[9] D. Mathivadhani, and C. Meena, "Digital Watermarking and Information Hiding Using Wavelets, SLSB and Visual Cryptography Method," IEEE International Conference on Computational Intelligence and Computing Research (lCCIC), pp.I-4, 2010.

[10] P.K. Sharma, and Ra jni, "Analysis ofimage Watermarking Using Least Significant Bit Algorithm," International ournal of Information Sciences and Techniques (mST) vol. 2, no. 4,2012.

[11] M. Fouad, A.E. Saddik, and E. Petriu, "Combining DWT and LSB Watermarking To Secure Revocable Iris Templates,"10th International

Conference on Information Sciences Signal Processing and their Applications (lSSPA), pp. 25 - 28, 2010.

[12] E. Mostafa , M. Mansour, and H. Saad , "Parallel-Bit Stream for Securing Iris Recognition," IJCSI International Journal of Computer Science Issues, vol. 9, no. 2, 2012.

[13] S. Edward, S. Sumathi, and R. Ranihemamalini, "Person authentication Using Multimodal Biometrics with Watermarking," International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), pp. 100 - 104,2011.

[14] K. Seetharaman, and R. Ragupathy, "Iris Recognition based Image Authentication," International Journal of Computer Applications, vol.44, no. 7,2012.

[15] M.Y. Sheng, Y. Zhao, F.Q. Liu, Q.D. Hu, D.W. Zhang, and S.L. Zhuang, "Acquisition and Pre-processing of Hand Vein Image," pp.5727 - 5729, 20