iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4641

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Embedding of Iris Data to Ear Image using Watermarking Technology, Pre-Processing Step

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

Abstract: ***Biometric acknowledgment or authentication is important procedure for acknowledgment of human in recent time. Here, a casual responsibility is biometric safety which is the secrecy issues derived from storage and misuses of the design data. In order to handle this point in question, researches have proposed different algorithms to be confronted by safety of biometric arrangements. Two important ways are, (1) Encryption, and (2) watermarking by securing biometric images and designs. In this paper, we avail a watermarking method to enhance the design or template safety in biometric confirmation or authentication. According to, two modalities such as iris, and ear is taken to maintain the traits of liveliness and continuity. Our proposed approach for embedding of iris data to ear image using watermarking technique to make better design security in biometric acknowledgment is done based on the pre-processing of iris, to ear image. Further we proceed this technique by iris template extraction, ear extraction, Embedding of iris pattern to ear image based on region of interest, and Storing embedded images. In the acknowledgment phase, iris motif is extracted from the embedded image and then, matching is done with concern images. The exertion is done using MATLAB.***

Keywords: Template; Watermarking; Embedding; Extraction; Authentication.

I. INTRODUCTION

Increased usage of electronic commerce and the opposing effects of terrorism have increased appliance of authenticating uses.

Todays, eyes have turned to use biometric ideas to meet the fulfillment. Biometric technique, which is a pattern acknowledgment technique, exploits a user's incomparable physical characteristics to identify/ acknowledge him/her. Two major groups of works that provide in a biometric system are labeling and acknowledgment. Biometric schemes considers various characteristics such as face, hand vein, gait, keystroke, odor, ear, fingerprint, face, hand geometry, retina, palm print, iris, voice and signature. Biometrics exhibits as an inherent tool when integrated. With established acknowledgment process that largely support in stablishing authenticity.

Some somber affairs that adhere with the biometric arrangement and data are their weakness against protection problems and adversarial attacks. Hence, fool-proof technologies have to be accepted to gain biometric motif, instead of using plain texts. Template based procedures in biometric scheme apply global-level processing to extract features after cropping particular sub-image from original sensory image. Biometric template can be generated with the aid of traits extractor or key binding algorithms. Such biometric templates can be kept secure and effectively protected by exploiting watermarking procedures. Biometric watermarking embeds biometric knowledge into a digital image and hence it correlates a person subjects with digital appliances. When key based embedding algorithm and pseudo noise techniques are used, digital watermarks can be predominantly inserted into the source data as transformed digital signal, through which the safety can be substantially improved. Watermarking can be said as a method of inserting crucial signals or messages which cannot be identified by humans. It can ensure multimodal biometric confirmation if the pattern is concealed with other biometric representation. It can be applied to safeguard the intellectual property rights by embedding information in the source data. However it is expected to be robust against some attacks against biometric arrangement.

Nevertheless, the increase in security needs have necessitates the research on developing permanent form of, irreproducible biometrics. One among such biometrics is iris of humans. Iris acknowledgment works on the basis of visual features such as rings, freckles, furrows and corona. Due to the high rate of randomness in such characteristics, iris confirmation is found to be very challenging. Further developments on infrared techniques that are observed in the present days, more accuracy can be accomplished by including more human traits, especially like probing ear, which are richer than fingers. This leads research concepts in iris, ear and face acknowledgment as one of hot spot areas in biometric confirmation. Patterns available in the ear are found to be distinctive between the individuals and remain same for long term throughout the human life. These vascular patterns are complex that lead to

determine ample feature sets to ensure precise personal identification. The researchers had discussed about various template security method and their importance in security of biometric template protection. Also, we found that there is need of robust biometric recognition technique for template protection. So here we design a biometric recognition system (pre-processing) by embedding iris data to ear image using watermarking technology.

The main contribution of the paper is, it propose a secure watermarking scheme to improve security of the templates used in biometric authentication.

II. PROPOSED EMBEDDING IRIS DATA TO EAR IMAGE USING WATERMARKING TECHNOLOGY

The aim of our biometric recognition system is to improve the template protection by embedding the iris data to ear images based on watermarking technology. The proposed technique of embedding of iris data to ear images using watermarking technology consist of following steps:

A. Iris 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.

B. 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.

C. Image Normalization

The next stage after iris segmentation is normalization to generate iris key and their comparisons.

D. Encoding

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

1) Ear image pre-processing and feature Extraction
2) Embedding of iris pattern to ear image
3) Recognition phase using score level fusion.

The algorithm we propose here is based on applying the Discrete Wavelet Transform (DWT) on the digital audio signal in which a watermark is to be embedded. The algorithm consists of two procedures watermarking embedding procedure and watermarking extraction procedure. The embedding procedure performs three major operations; watermark pre-processing, DWT-based decomposition, and watermark embedding in the DWT-transform. In this paper we only defined the pre-processing step. The pre-processing step include the following step:

a) *Load Image*- In this step we load an image which is our ear image.

Figure 1: An ear image taken as load image

b) *Sample image* – In this step we take a sample image which is iris image, given below:

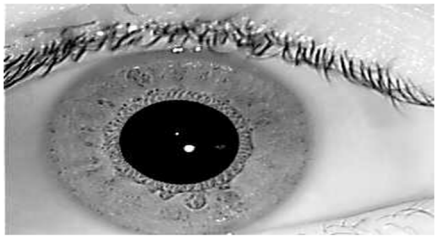


Figure 2: An iris image taken as sample image

c) Encrypted Image – In this step we encrypt the sample image which is iris image into load image which is ear image.
d) Scrambled Image – Now, scrambled the encrypted ear image.
e) Compressed Image – In this process we compressed two image.
Wavelets are special functions which, in a form analogous to sines and cosines in Fourier analysis, are used as basal functions for representing signals. They provide powerful multi-resolution tool for the analysis of non-stationary signals with good time localization information. The coefficients of the discrete wavelet transform can be calculated recursively and in a straight forward manner using the well-known various algorithm. Based on various algorithm, the one- dimensional discrete wavelet coefficients of any stage can be computed from the coefficients of the previous stage.

III. RESULTS AND DISCUSSION

In this section we analyzed and discussed about the proposed technique.

A. Experimental Setup and Evaluation Metrics

We had implemented the proposed method using MATLAB. Also, the evaluation metrics used here is the accuracy. The accuracy in multimodal biometric is computed based on FAR (False Acceptance Rate) and FRR (False Rejection Rate).

B. Experimental Result

The following figures shows the results of pre-processing steps are as follows:

1) Load Image

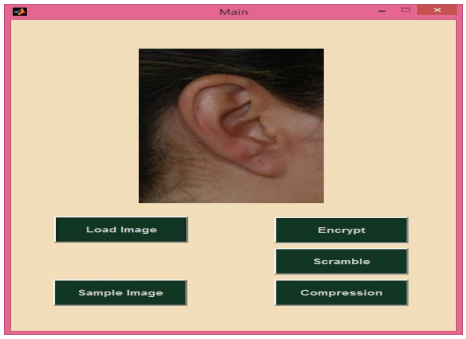


Figure 3: loaded ear image in the pre-processing stage

2) Sample Image

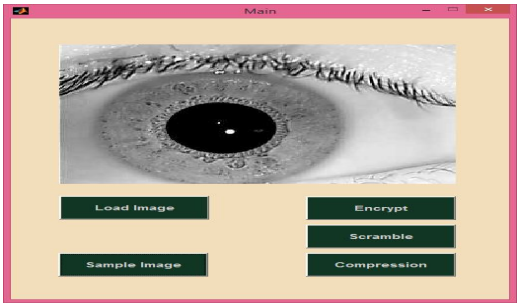


Figure 4: An Iris Image which is taken as sample image in the pre- processing stage

3) Encrypt Image

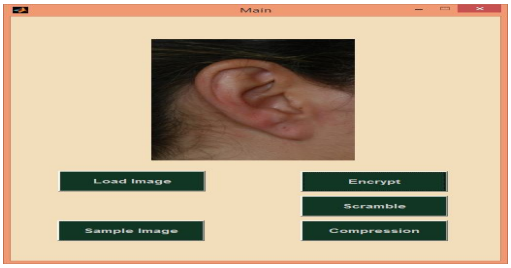


Figure 5: Encryption of sample image in the loaded image

4) Scramble Image

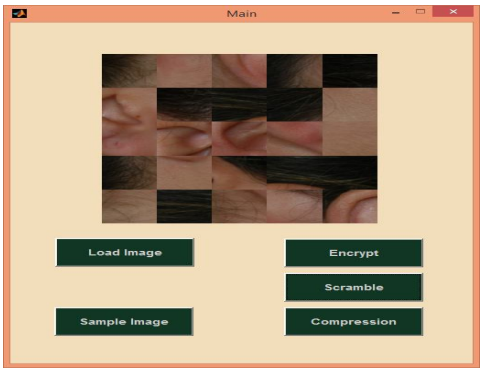


Figure 6: The scrambled image

5) Compressed Image

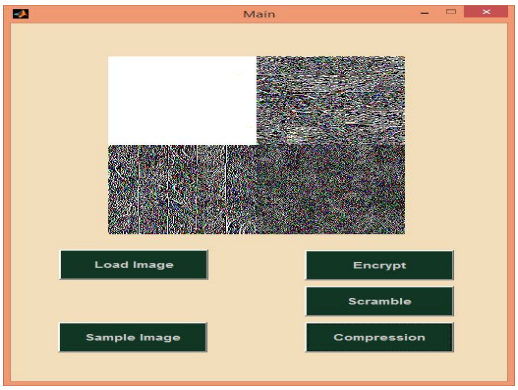


Figure 7: compressed image

IV. CONCLUSION AND FUTURE SCOPE

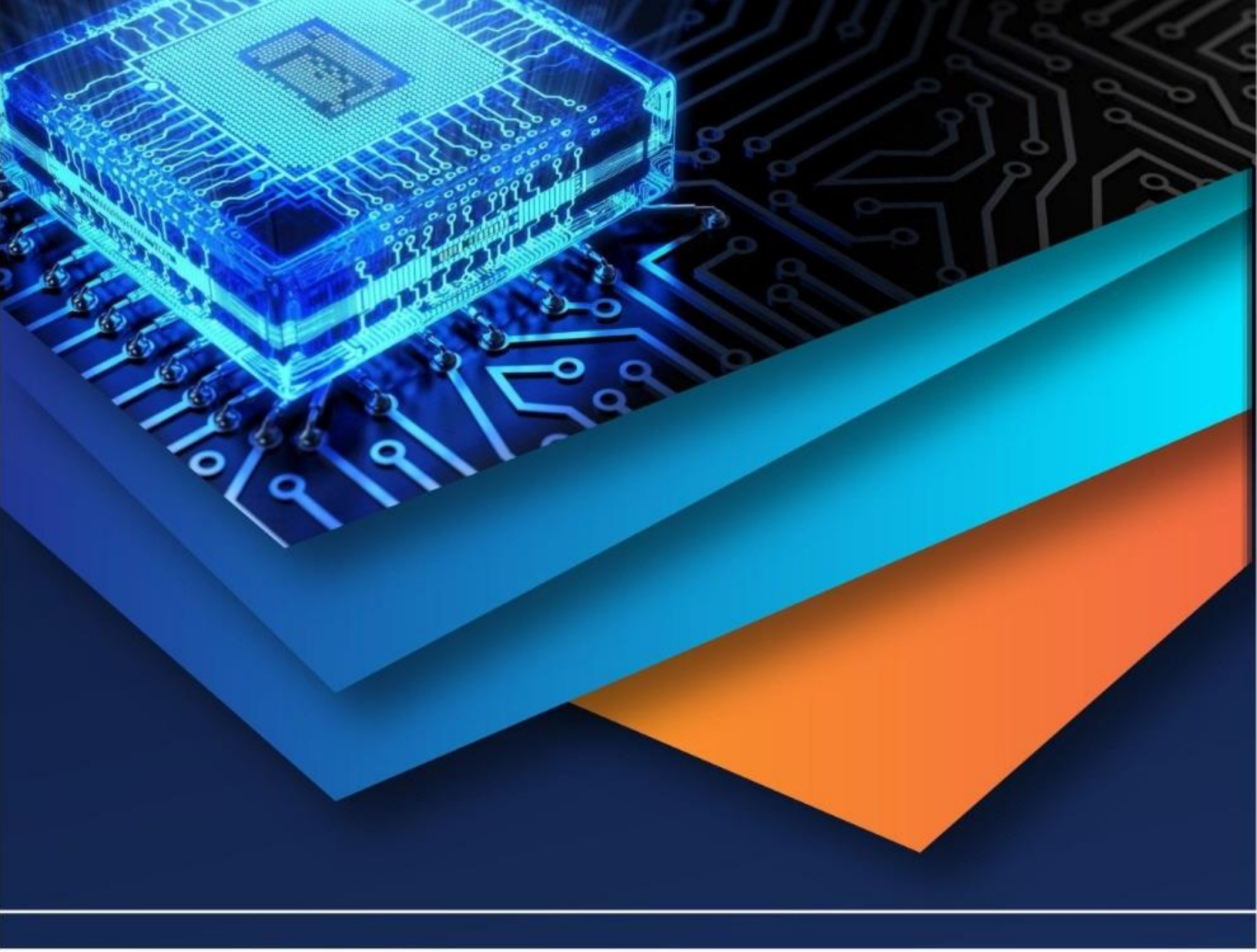
In this paper, we have presented an efficient biometric recognition for template protection pre-processing stage. We have used a watermarking technology to improve the template protection based on the two modalities the iris and ear. In the pre- processing step we load an image first, then take a sample image and encrypt it with the load image. After that we scramble the encrypted image and finally compressed it foe security.

We can improve this work by the feature extraction, embedding and matching process. We can also use the different human traits and different algorithm or multi algorithm techniques and calculate various performance parameters. Apart from that the accuracy of our proposed method can be further improved by improving the embedding strength and embedding location by various search algorithms.

REFERANCES

[1] P.S. Revenkar, A Anjum and W.Z. Gandhare, "Secure Iris Authentication Using Visual Cryptography," International Journal of Computer Science and Information Security, vol. 7, no, 2010
[2] AK. Jain, A Ross, and U. Uludag, "Biometric Template Security Challenges and Solutions," In Proceedings of European Signal Processing Conference, 2005.
[3] 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
[4] 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
[5] 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
[6] 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 (ICCIC), pp.I-4, 2010
[7] P.K. Sharma, and Rajni, "Analysis ofimage Watermarking Using Least Significant Bit Algorithm," International Journal of Information Sciences and Techniques (mST) vol. 2, no. 4, 2012
[8] 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

[9] 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
[10] K. Seetharaman, and R. Ragupathy, "Iris Recognition based Image Authentication," International Journal of Computer Applications, vol. 44, no. 7, 2012
[11] 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 II
[12] M.M. Pal, and R.W. Jasutkar, "Implementation of Hand Vein Structure Authentication Based System," I nternational Conference on Communication Systems and Network Technologies, pp. 114 - lIS, 2012
[13] Sanchit, M. Ramalho, P.L. Correia, and L.D. Soares, "Biometric Identification through Palm and Dorsal Hand Vein Patterns," International Conference on Computer as a Tool, pp.I-4, 20 I I
[14] R.M. Thanki, and K.R. Borisagar, "Novel Approach For Multimodal Biometric System Using Compressive Sensing Theory Based Watermarking," International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), vol. 3, no. 4, pp. SI- 90, 2013
[15] A Bamatraf, R. Ibrahim, and M.N. Salleh, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit," Journal of Computing, vol. 3, no. 4, 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY