ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Robust Security Using Multimodal Biometric Key Along With GSM

Raji Pandurangan, Dr. M. Sundararajan*
Department of ECE, Bharath University, Chennai,
***Corresponding author: E-Mail:msrajan69@gmail.com**

ABSTRACT

In this era the advance growth in technological field regarding security purpose has brought people at a summit where they can take a sigh of relief against plagiarism. The main cause behind this is the multimodal biometric feature based systems which are becoming predominant in larger scale security based applications because they have many advantages such as error reduction and higher population coverage if we compare them to single biometric based systems. The vast majority of computerized watermarking algorithm have been presented, yet they are vaporous because of the balance between credit execution and security of the format. This paper evaluates the main literature related to the multiple biometric based digital watermarking which is presented with GSM module based on embedded technique for more security using one time password within the system

KEYWORDS: Multimodal biometric, Single biometric Watermarking, Security, GSM module.

1. INTRODUCTION

In this 21st century where we observe plagiarists, intruders and cyber-terrorists using the information of other people to get their secure information where billions of bits of data is developed and destroyed in a bit of a second and with the advent of internet, transmitting and receiving of digital data (images as well as videos moreover audio files, digital sources collections and web publishing) has developed many fold. Amid the reproduction of a digital Data is very easy and loose besides so, issues like, protection of moralities of the data and proof of ownership arises. Then to verify and secure transmission digital watermarking technique and a tool to copyright laws for digital data has presented. The zone of watermark is that it remains achieve to the shelter work regardless of the possibility that it is replicated. So to demonstrate power of own information getting end watermark is decoded and confirmed. It is hard for reprobate to kill or change watermark. In that capacity the genuine proprietor can simply have his information sheltered and secure.

Multi-bio-metric recognizable proof frameworks have as of late picked up enlistment from the examination group, following these have been utilized as a part of a few beneficial applications, for example, reconnaissance and access control against impostors, secure data management. Multimodality is another and quickly developing subject examination in biometrics field in the fast world. Multimodal biometric framework is a sort of example pattern recognition, which recognizes an individual in physiological or behavioral properties, similar to that face discovery unique mark are recognition and other palm vein recognition. A multimodality idea is said, where separated from combination various attributes procedure proposed. In joined element recognition of iris and face biometrics proposed. The score level and coordinating of their combination in multimodal biometrics framework proposed in. So as to perceive people, these frameworks are more wanted to one biometric highlight. These frameworks give higher acknowledgment rate when contrasted with uni-biometric frameworks transfer on one and only biometric in this running world, multimodality is another and quickly developing exploration in the biometrics field. Multimodal biometric framework is a sort of example recognition framework, which distinguishes an individual taking into account physiological or behavioral properties, similar to that face discovery unique finger impression acknowledgment and other palm vein acknowledgment. The main aim of this paper to study different watermarking techniques with the use of embedded based GSM module technique which provide maximum security for users and owners.

Watermarking from Multiple Subjects and Reviews: This paper comprises of computerized watermarking based secure multimodal biometric (unique mark and iris) framework in which double parts of security are present for verifying any individual and serving the biometric formats. This system use mainly DWT (discrete wavelet transform) and IDWT (inverse discrete wavelet transform) based algorithm. This watermarking algorithm gives higher security. Once the system is affected by the outer intermediate attacker then biometric templates will not be replaced.

By and large multimodal biometric picture watermarking is done utilizing dual stage respectability confirmation. This paper, gives multimodal biometric picture watermarking plan through a double uprightness verification system utilizing the mystery abrupt element vectors for safe approval of multimodal biometrics information, iris and unique mark, individually. It is for the most part taking into account shade and spread range based solid watermarking system. This technique empowers to recognize an altered locale by keeping up watermark inserting specialty to meet the prerequisite of predefined watermark through transmission of information extraction edge. The thought is that the thumbnail highlight vectors of an iris picture as a watermark example are utilized by embedding's as a part of a unique mark in order to review the dependability of individual biometric information. The primary phase of honor confirmation for a unique finger impression picture is finished by deciding the legitimacy of

removed thumbnail designs. The phase of joined validation for an iris picture is finished by coordinated coordinating between the thumbnail highlight vectors derived from an iris picture and the thumbnail one of the got iris picture. This paper, clears up the spatial space based solid biometric picture watermarking strategy utilizing 2-stage trustworthiness confirmation technique which recognize the prudence of biometric information utilizing emitted thumbnail highlight vectors for security reason. Here in, fingerprints and iris biometric information are utilized for multimodality plan. These two biometric information are caught and telecasted to the biometric confirmation framework. The terse component vectors of the iris picture are just watermarked into the unique mark picture as a spread picture watermark for information concealing reason before transmission. At that point, at the accepting or verification framework, the honesty inside of the blend of logo picture and additionally cover picture at first unique finger impression picture is checked by checking the legitimacy of thumbnail highlight vectors (watermark) executed utilizing a predefined watermarked extraction limit. Thereafter, the thumbnail highlight vectors removed from a watermarked unique finger impression picture is identified with the abrupt ideals of the first iris picture to verify the honesty of the iris picture. From this distinguishing proof of the consolidated iris and in addition unique mark picture is finished.

To implant the watermark utilizing biometric elements particularly change area watermarking plan, for example, quick Fourier change (FFT), discrete cosine change (DCT) discrete wavelet transform(DWT) and Radon change can be connected. It is surely understood that the change space watermarking method has exactness and preferable execution over the spatial area watermarking plan. Be that as it may, if the power is completely concurred then spatial area watermarking plan is superior to anything recurrence based one on the grounds that it is less demanding and fast.

Individual Recognizers: In advanced watermarking fundamentally perceive that iris and unique finger impression biometrics performance are great when contrasted with other strategy. These qualities make iris and unique finger impression acknowledgment especially proofs for better security for society. The procedure begins with preprocessing of the got pictures which find the commotion impact. Further, elements are gathered from testing pictures and contrasted with discover the closeness between two element attributes. The coordinating scores which are obtained from the each recognizers are connected to the handling module where a man is announced as confirmed or not by applying one time secret key utilized by the validated individual on the off chance that it is legitimate then he is indicated verified if not then unapproved.

Iris recognition: The iris is an annular ring exists the sclera and understudy limit and have the ring example unmistakable to every person. The coordinating calculation is utilized to produce grid type of diverse pixel between the database and question pictures of iris. The standard of multi-scale quadrature wavelets is utilized to concentrate surface stage structure subtle elements of an iris, to produce a 2048 piece iris code and thinks about the iris pair representations contrast by figuring their Hamming separation utilizing XOR administrator. For this situation for the most part the zero-intersection representation of 1-D wavelet change at numerous determination levels of a certain circle on an iris picture to portray the composition of an iris has been processed. The essential steps included in iris acknowledgment fundamentally are: Pupil, Iris detection, Normalization, Feature Extraction, and Matching.

The pixel position has the higher worth in the range picture compares to the student focus. The range is characterized by the student is the separation towards the understudy focus and closest pixel that has no zero.

Iris Detection: The mapping is done in the wake of changing the Cartesian coordinates into its polar proportionate utilizing Matlab picture preparing device and the correlation is done between iris codes produced for database and question pictures performed by for the most part hamming separation strategy. In this methodology the distinction between code bits got are measured and the value is partitioned by the aggregate examination's number.

$$MS_{Iris} = \frac{1}{N}\sum_{i=1}^{N} A_i \oplus B_i$$

Where double vector (iris code) is an is for the database picture and twofold vector for concern picture is B, and N is the quantity of components. This coordinating score (MSIris) is utilized as information for the part where the end coordinating score is delivered with unique mark score esteem.

Fingerprint Recognition: Unique mark is one of the significant biometric human body highlight. Let the examples of chine and valleys on the highest point of the finger. The real strides in unique mark acknowledgment utilizing details coordinating technique after picture obtaining are:

- Image Enhancement
- Minutiae Extraction
- Matching

Image Enhancement: A unique mark picture gets to be pointless because of various types of clamors, for example, gaps, smirches and wrinkles. It is exceptionally hard to recoup the genuine edge/valley life systems from the non-reachable districts, any push to develop the nature of the unique mark in these area are vain. The information of pre-

determined mean and difference of standardized data unique finger impression picture are utilized to create score esteem by utilizing Matlab. Further, recurrence picture is figured from the standardized info unique mark picture and the evaluated introduction image.

Minutiae Extraction: The upgraded unique finger impression picture is doubles and prepared by diminishing calculation that which lower the bar thickness to one pixel wide. The area of details focuses alongside the introduction is removed and put away utilizing picture handling device with the assistance of Matlab. For extraction of details point eight associated pixels are utilized. The Crossing Number system is utilized to perform particulars extraction. The CN for a pixel ridge denoted as Pis given by

$$CN = 0.5\sum_{i=1}^{8} | P_i - P_{i+1} |$$

$P_9 = P_1$

Where *Pi* is called as pixel value in the around *P*. *T*hen crossed no. for a ridge pixel has been calculated, the pixel can then be sort into its crossed no. value.

Matching: The database and inquiry unique finger impression pictures are utilized for test extraction and considered as focuses in the 2D plane for the most part as 0 and 1s structure for less demanding extraction and era of score quality. A minutia based coordinating contains arrangement between the organization and the data sets that outcomes in the more number of exact pair. Taking variable D = {m1… … mm} and C = {m1… … .mn} be the set that are acquired from question and database pictures in like manner. Where m={x,y,θ}, x and y are the directions at that specific particulars point and introduction is θ. Blending is done utilizing

Particulars in an and details in B are thought to be coordinated if the spatial separation between them is littler than a given resistance r0 and the dd between them is littler than a rakish resilience indicated as θ0. The coupling encourage a closeness score (MSFinger) which is prepared.

Combination: No other biometric highlight can give 100% precision. Further, the outcomes produced from them are great yet the issue emerges when the client is not ready to give his iris picture because of trouble in introduction to light Similarly, the issue happens by unique finger impression acknowledgment framework is the vicinity of cuts and scars. This all add commotions to the unique finger impression picture which can't be eradicated effortlessly by module. In this way, the framework takes uproarious unique mark as data which is not ready to reason the particulars focuses precisely and thusly, prompts bogus acknowledgment of a person. In this manner to get over the issues confronted by individual qualities of iris and unique finger impression, a novel blend is presented for the acknowledgment framework. The coordinated framework additionally gives an against hardening so as to satirize measures it for an interloper to farce numerous biometrics. Scores started from individual qualities are forced at coordinating score stages with the assistance of weighted total the procedure. Let MSIris and MSFinger be the coordinating scores got from utilized qualities individually. The strides are

Score Normalization: This stride brings both coordinating scores somewhere around 0 and 1 utilizing Matlab programming. The standardization of both the scores are finished by

$$N_{Iris} = \frac{MS_{Iris} - \min_{Iris}}{\max_{Iris} - \min_{Iris}}$$

$$N_{Finger} = \frac{MS_{Finger} - \min_{Finger}}{\max_{Finger} - \min_{Finger}}$$

Where minIris and maxIris are iris acknowledgment least and most extreme scores and minFinger and maxFinger are the relating qualities got from unique finger impression acknowledgment.

Generation of Similarity Scores: The standardized score gives the comparative estimation of both attributes coordinating score. So to wire both the score, we have to make both the scores in standardized example. In this paper, iris standardized score is changed. $N'_{Iris} = 1 - N_{Iris}$

Watermarking After Fusion: The two scores N'Iris and NFinger are intertwined single dimensionally utilizing whole lead as

Where α and β are two weighted qualities. On the off chance that the benefit of coordinating score is not as much as limit then the weight is doled out straightly, else exponential weight is offered significance to the score.

The benefit of coordinating score is utilized to watermark both the characteristics. So if coordinating score is observed to be more than the given limit esteem the applicant is approved if not then reject. The SVD (single valued decomposition) based algorithms mostly applied in image processing and visualization it operates only on a positive matrix. The cover image in the form of a matrix (as secret information like audio, video, documents) matrix split as 3 sub matrix by SVD and watermark image summed with cover image matrix. Then produced watermarked image with the help of discrete wavelet transform method at the transmitting section. The decomposition technique

is involved in the watermarked image and at this instant GSM module is used for the accurate security option, after decomposition there is random password generation with the use of GSM module and this password is used for authentication purpose at the receiving end. Finally the watermark image (consisting of both the traits fingerprint as well as iris is) decrypted from cover image this method. This system gives the very good image stability and intrinsic algebraic image properties.

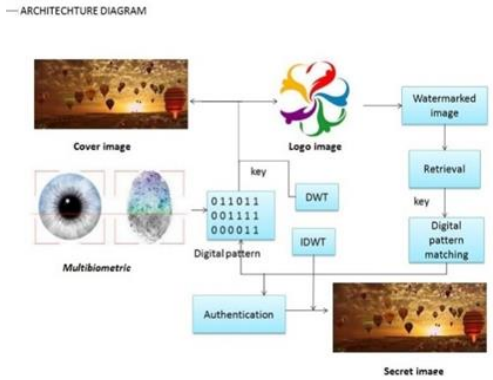

Figure.1. Architecture Diagram

Compressive sensing theory based watermarking system: This systems generate the measurement vector about the watermark templates using the image transformation and measured matrix and measured vectors incorporated on cover image the confidentiality becomes tough as restoring secure biometric template is very difficult from measurement vector without the samples of original measurement matrix and image transformation.

Modified Correlation based system: This watermarking system uses modified correlation watermarking algorithm. The iris code is watermarked into fingerprint image using secret key. Before watermarking the cover image is pre-processed by using pre filtering techniques, this increases the high result correlation. Iris is taken as watermark on fingerprint image. A pseudo random noise which is additive is applied to the biometric templates for watermark embedding.

2. EXPERIMENTAL RESULT

The outcomes are executed on iris and unique mark pictures gathered by the creators. The database comprises of one iris picture (200×3) and one unique mark picture (200×3) per individual. The iris picture is obtained utilizing CCD camera with uniform light source. Unique mark picture are obtained by utilizing an optical unique finger impression scanner. There two levels of trials are performed for the reason permitting correlations. In initial step fingerprints and iris calculations are tried independently. At this stride the individual results are processed and a precision bend is plotted which is appeared in Figure 2. In this level the iris and unique finger impression precision is observed to be 94.36% and 92.06% individually, appeared in Table 1.

At second level the coordinating scores from the individual qualities are consolidated and last precision diagram is plotted, appeared in Figure 3. In Table 1 the exactness and mistake rates acquired from the individual and consolidated framework. So now the general execution of this framework has expanded an exactness demonstrating 96.04% with FAR of 1.58% and FRR of 6.34% individually. It is clear from the plot that the incorporated framework is giving most noteworthy GAR at least FAR. Histograms for real and fraud information, appeared in Figure 4 beneath. The authentic and sham information circulation demonstrates that the framework gives greatest exactness of 96.04% least FAR and FRR rates with at edge of 0.5. After this fusion experiment both traits act like a logo image and then the secret data is imposed on logo image for secure transmission purpose. This whole process is done for the used authorization and secure data management.

Table.1. Figures indicating individual and joined precision

Trait	Algorithm	Accuracy (%)	FAR (%)	FRR (%)
Iris	Haar Wavelet	94.36	4.85	6.43
Fingerprint	Minutiae Matching	92.06	3.17	12.69
Fusion	Haar + Minutiae	96.04	1.58	6.34

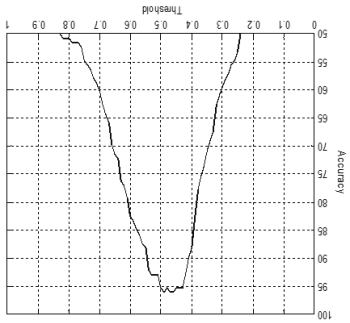

Figure.2. Accuracy chart for joined classifier

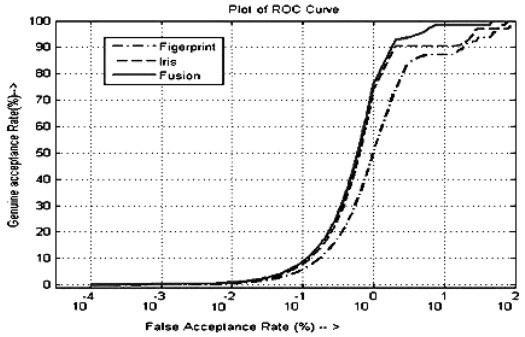

Figure.3. ROC Curve for Fingerprint, Iris &Fusion

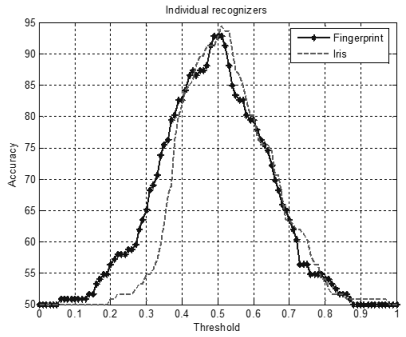

Figure.4. Accuracy plots of individual recognizers

3. CONCLUSION

The paper presented a biometric individual verification framework utilizing the gathering of iris and unique mark. One methodology is utilized to get over the impediments postured by the other methodology. The exploratory result demonstrates that the exactness of framework would raise on consolidating the qualities. It gives a general precision of 96.04% with FAR and FRR of 1.58% and 6.34%. Multimodal biometric watermarking budding research area that has occupied great profit from the research community over the last years. Here, existing researches that are robust against intruders are investigated. An introduction about the multimodal watermarking is obtained by new method to generate random password using GSM module is proposed to maintain the system more secure as well as accurate. These review overlays the way to the potential researchers to know about the various techniques available for Biometric watermarking

REFERENCES

Dass S.C, Nandakumar K & Jain A.K, A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA*)*, Rye Brook, NY, 2005.

Daugman J.G, High confidence visual recognition of persons by a test of statistical independence, IEEE Transactions on Pattern Analysis and Machine Intelligence, *15*(11), 1993, 1148–1161.

Fusion of Iris and fingerprint biometric for recognition base paper taken from IIT Kanpur published paper.

Gopalakrishnan K, Sundar Raj M, Saravanan T, Multilevel inverter topologies for high-power applications, Middle - East Journal of Scientific Research, 20(12), 2014, 1950-1956.

Hong L, Wan Y & Jain A.K, Fingerprint Image Enhancement, Algorithm and Performance Evaluation, IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(8), 1998, 777-789.

International Journal of Applied Engineering Research (IJAER), 24(9), 2014, 25835-25839.

Jain A.K, Nandakumar K & Ross A, Score Normalization in multimodal biometric systems. The Journal of Pattern Recognition Society, 38(12), 2005, 2270-2285.

Jasmin M, Vigneshwaran T, Beulah Hemalatha S, Design of power aware on chip embedded memory based FSM encoding in FPGA, International Journal of Applied Engineering Research, 10(2), 2015, 4487-4496.

Kanniga E, Selvaramarathnam K, Sundararajan M, Kandigital bike operating system, Middle - East Journal of Scientific Research, 20(6), 2014, -685-688.

Kanniga E, Sundararajan M, Modelling and characterization of DCO using pass transistors, Lecture Notes in Electrical Engineering, 86(1), 2011, 451-457, 2011.

Karthik B, Arulselvi, Noise removal using mixtures of projected gaussian scale mixtures, Middle - East Journal of Scientific Research, 20(12), 2014, 2335-2340.

Karthik B, Arulselvi, Selvaraj A, Test data compression architecture for low power vlsi testing, Middle - East Journal of Scientific Research, 20(12), 2014, 2331-2334.

Karthik B, Kiran Kumar T.V.U, Authentication verification and remote digital signing based on embedded arm (LPC2378) platform, Middle - East Journal of Scientific Research, 20(12), 2014, 2341-2345.

Karthik B, Kiran Kumar T.V.U, EMI developed test methodologies for short duration noises, Indian Journal of Science and Technology, 6(5), 2013, 4615-4619.

Karthik B, Kiran Kumar T.V.U, Vijayaragavan P, Bharath Kumaran E, Design of a digital PLL using 0.35Î¼m CMOS technology, Middle - East Journal of Scientific Research, 18(12), 2013, 1803-1806.

Lee H.C, & Gaensslen R.E, Eds, Advances in Fingerprint Technology, New York, Elsevier, 1991.

Philomina S, Karthik B, Wi-Fi energy meter implementation using embedded linux in ARM 9, Middle - East Journal of Scientific Research, 20(12), 2014, 2434-2438.

Raji Pandurangan, Loganshanmugam E, DCT-SVD and DWT-SVD Image Watermarking Techniques, in

Raymond Thai, Fingerprint Image Enhancement and Minutiae Extraction, Technical Report, The University of Western Australia, 2003.

Ross A & Jain A.K, Information Fusion in Biometrics, Pattern Recognition Letters, *24*(13), 2003, 2115-2125.

Saravanan T, Sundar Raj M, Gopalakrishnan K, Comparative performance evaluation of some fuzzy and classical edge operators, Middle - East Journal of Scientific Research, 20(12), 2014, 2633-2633.

Saravanan T, Sundar Raj M, Gopalakrishnan K, SMES technology, SMES and facts system, applications, advantages and technical limitations, Middle - East Journal of Scientific Research, 20(11), 2014, 1353-1358.

Vandana sinamdar and pritirege, Dual watermarking technique with multiple biometric watermarks,Indian Academy of Sciencess, 39(1),2014, 3-26.

Vijayaragavan S.P, Karthik B, Kiran Kumar T.V.U, A DFIG based wind generation system with unbalanced stator and grid condition, Middle - East Journal of Scientific Research, 20(8), 2014, 913-917.

Vijayaragavan S.P, Karthik B, Kiran Kumar T.V.U, Effective routing technique based on decision logic for open faults in fpgas interconnects, Middle - East Journal of Scientific Research, 20(7), 2014, 808-811.

Vijayaragavan S.P, Karthik B, Kiran Kumar T.V.U, Privacy conscious screening framework for frequently moving objects, Middle - East Journal of Scientific Research, 20(8), 2014, 1000-1005.

Yunhong W, Tan T & Jain A.K, Combining Face and Iris Biometrics for Identity Verification, Proceedings of Fourth International Conference on AVBPA, Guildford, UK, 2003, 805-813.