# Secure Multimodal Biometric Authentication System against Spoofing Attacks

[1]S.G.Adlin Nisha, [2]Dr.M.K.Jeyakumar
*[1]M.Phil Computer Science, [2]Dept of Software Engineering*
*Noorul Islam Center for Higher Education*
*Kumaracoil*
*Thuckalay-629180*

***Abstract***

*Anti-spoofing is appealing rising attention in biometrics, since the variation of imposter resources and fresh incomes to attack biometric recognition schemes. Different unnoticed things incessantly test state-of-the-art spoofing sensors, signifying for further methodical methods to goal anti-spoofing. By integrating liveness marks hooked on the biometric synthesis development, credit accurateness container remain improved, nonetheless likelihood ratio founded synthesis algorithms are identified to be extremely searching to only spoofed cases. In this research, address the safety of multimodal biometric schemes when one and only of the methods is positively spoofed. Here propose dual novel fusion schemes that can upsurge the safety of multimodal biometric schemes. The beginning is the extension of the likelihood ratio based fusion scheme and the further uses fuzzy logic. Also the matching score and taster excellence score, our proposed fusion schemes also take into explanation the intrinsic safety of each biometric scheme being bonded. New consequences have exposed that the proposed approaches are more robust against spoof attacks when likened with traditional fusion approaches.*

**Keywords -** *Presentation attacks, safe multibiometric fusion, Biometrics, security.*

## I. INTRODUCTION

Numerous different kinds of biometric characters can be recycled to accomplish programmed individual verification (e.g. impression, look, speech, pointer geometry, etc.). The biometric features charity in a verification procedure wants to chance certain elementary necessities like universality, uniqueness, durability, among others [1]. Though, in applied

Applications, no biometric typical completely encounters these fundamentals, accordingly no lone biometric style for free of mistakes. Specific of these limits container be overpowered or diminished unknown multiple biometric modalities remain rummage-sale.

Trendy instruction toward income complete improvement of the multimodal method, it is indispensable to instrument a decent technique for combining dissimilar foundations of biometric material. Numerous synthesis approaches obligate presence freshly future [3–5], existence that all them show that multimodal biometric schemes can meaningfully upsurge the acknowledgment charges once likened to unimodal biometric schemes. However, nobody of these have been traveled the security topics, which is the attention of this research.

Instinctively, a multimodal scheme is essentially more safety than unimodal schemes since it is additional problematic to spoof two or other biometric characters than a solitary one. Though, is it actually essential to spoof all the bonded biometric characters to blow a multimodal scheme? This question is significant when a very protected biometric (e.g retina scan) is joint with additional that is effortlessly spoofed (e.g. face). In this situation, the welfares of addition the face info may be annulled by discount in general safety.

The likelihood ratio (LLR) between the honest and deceiver delivery is recognized to be the ideal fusion technique, in the intelligence that it reduces the likelihood of mistake [6, 7]. This shoulders are representative estimate for both deliveries is obtainable, which typically is educated from working out data. For example, in [6], a Gaussian mixture model is used to model these deliveries. Though, these deliveries are erudite deprived of seeing the theory that an fake user might have spoofed a biometric style meanwhile lone ‘‘non-spoofed’’ fake tasters are used in the working out procedure. The faintness of a fusion system accomplished this way will only demonstrate up in a situation when a biometric mode was positively spoofed.

Certain new researches have planned the outline of supplementary info, similar biometric taster superiority [2–4] then operator explicit limitations [5], popular the synthesis process to shape additional flexible and dependable biometric schemes. The overall impression now these approaches is to ‘‘weight’’ (straight before circuitously) the influence of all unimodal biometric founded on the supplementary info. At this time discover a comparable idea through combination in the synthesis procedure auxiliary info that specifies how safe each biometric style is. Our leading impartial is to grow biometric fusion plans that are healthy in contradiction

of spoof occurrences and that remain accomplished of joining biometric schemes with dissimilar heights of safety deprived of cooperating the general safety of the multimodal scheme.

In this research, suggest dual original multimodal biometric synthesis systems that deliberate the spoofing theory then income hooked on explanation the safety of every biometric scheme presence attached. The chief system is an postponement of the LLR and the another is demonstrated by fuzzy logic. Together replicas segment the similar elementary designs; nonetheless vary in particulars and execution

## II. RELATED WORKS

There are numerous anti-spoofing or liveness discovery algorithms removing structures (usually trained for modality, sensor, material, etc.), in order to define whether a biometric taster is whichever real or fake. For assessment determinations, rate of misclassified live models and degree of misclassified fake tasters are working. While for separate modalities the anti-spoofing tricky is well distinct and assessed distinctly from biometric scheme presentation, investigation on combination among competition scores and livenss issues is motionless in its beginning [16]. Lately, [17] optional a background for confirmation schemes under spoofing attacks. Inside the agenda [16] accepted in this research, liveness and acknowledgment grooves are joint seeing the situation of probe-spoofing alone (i.e. not at all gallery-spoofing, compulsory by e.g., joined staffing).

### *A. Combining recognition and anti-spoofing*

Marasco et al. [10] remain amongst the major seeing fusion of liveness through credit scores distinctly aimed at every modality, by humble refusal of spoofed tasters. Unknown a spoofing effort is designated; the present modality matching slash is overlooked. This main education is protracted in [15] assessing consecutive synthesis, classifier synthesis, then Bayesian Belief Systems for marrying match scores and liveness events, importance the advantage of the final technique for the LivDet2009 dataset nonetheless too that correctness is reduced once captivating liveness discovery hooked on explanation. Chingovska et al. [11] assess dual choice instructions and Logistic Regression (LR) as choice then score-level synthesis methods joining face credit and liveness notches speaking the addition (nonetheless abandoning the incomplete spoofing problematic) of liveness. Stated advanced confrontation to spoofing attacks (91.54% vs. 10%) but are outstripped by LR methods attaining both, high confirmation accurateness and upright spoofing discovery. Recently, Poh et al. [12] have beleaguered the problematic of assimilating spoofing and matching scores in a probe and gallery spoofing scenario, examining Gaussian Copula-based Bayesian classifiers and a combination of linear classifiers for this mission. While their technique outclasses traditional Support Vector Machine (SVM) founded methods, the method needs exercise with respects to the filled variety of attacks. The valuation of traditional fusion rules (this work is using Kittler et al.'s classical framework [16]) in the attendance of spoofing attacks is a additional pertinent sub-problem and spoke in this research. Rodrigues et al. [13] first spoke this safety subject of spoofing attacks in contradiction of a multimodal biometric scheme. I proposed the binary approaches, unique by likelihood proportion then additional paying fuzzy logic, together beyond the correctness of outdated synthesis rubrics. Also Akhtar et al. [14] deliberate the influence of spoofing on similar and sequential synthesis rubrics for face and fingerprint commentary that score-level fusion approaches after that works remain not healthy to spoofing attacks then that sequential synthesis provided improved consequences aimed at a general valuation of presentation, confirmation period, operator suitability then heftiness

### *B. Anti-spoofing in fingerprint and face recognition*

Now fingerprint credit, here is a binary universal habit there is discourse the spoofing problematic: whichever by aggressively measuring the liveness (e.g. through gauging beat, sweat designs, otherwise blood weight), otherwise through inertly examining designs of spoofed resources (e.g. nonexistence of part, design changes). The last kind, which is the topic of attention in this research, discloses in height danger of physical and sensor-dependence. An outstanding current review of spoofing approaches in fingerprint credit can be found. Amongst the greatest mutual methods for still (removed since solitary image) texture-based anti-spoofing approaches are arithmetical topographies, Control Range Fourier examination, Point Incidence Examination, Local Binary Patterns (LBP) and Local Phase Quantization. Though, fresh growths just before material-independent stationary anti-spoofing propose to syndicate multiple topographies then perhaps smooth sensors. Fumera et al. [16] stretch a decent outline hooked on the problematic of uniting multiple liveness sensors aimed at a lone modality, synthesis of liveness sensor then matcher aimed at a solitary modality, then anti-spoofing competences of ad hoc synthesis procedures uniting multiple contrast slashes.

Face spoofing counter-measures container approximately be secret hooked on texture-based and motion-based counter-measures. A decent impression on face counter-spoofing might be originated in [18]. The chief group measuring textural possessions is the additional extensive collection through methods similar LBP before arithmetical geographies abusing the comment that images/videos by spoofed faces (published before repeated) prepare not exhibition the similar noise-level similar honest tasters. The kind of motion-based methods goals the imitation of (level) published pictures or re-display of faces on medicines misusing the alteration in 3D entrance of spoofed

methods. Aimed at synthesis determinations this research emphasis on the chief kind then employments a present anti-spoofing scheme.

## III. SYSTEM ARCHITECTURE

As shown in Fig. 1, the system architecture of our proposals contains of enterprise stage and connected stage.

The research,on multibiometric systems exploiting score-level fusion to combine the matching scores coming from K distinct biometric traits. Throughout the plan stage approved customers are joined by storage their biometric characters (i.e., templates) and individualities in a folder. Through the connected procedure, each user brings the required biometrics, and privileges the independence of an authorized customer. The reliable patterns are improved from the record and matched in incongruity of the submitted types. The matching scores s = (s1, . . . , sK) ∈ $R^K$ are joint ended a fusion regulation which productions an joint notch f(s) ∈ R. The joint score is to accomplish related with a edge t to select whether the independence true is comprehensive through a true operator (if f(s) ≥ t) before an false. Presentation remains measured, by way of aimed at unimodal arrangements, by predicting the False Acceptance Rate (FAR) then the False Rejection Rate (FRR) after the honest then fake deliveries of the combined notch [22].

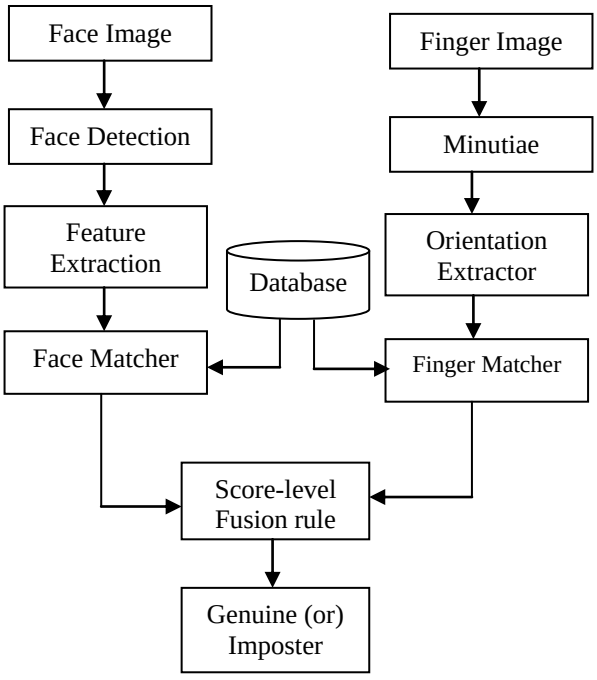


**Fig.1. System Architecture**

## IV. PROPOSED WORK

In proposed work, multimodal biometrics uses material from two or more biometrics. Here, a user records into the scheme by means of face and fingerprint. In design phase, authorized customers are registered by storage their biometric traits and characteristics in a file. In online process, user delivers demanded biometrics, and rights the individuality of an authorized customer.

### *A. Face Matcher*

This module obtains the face biometric data since a user and rights his individuality. This component, attain the face discovery on each of these images. Thus, given a image is carry out the face detection by retaining the Viola-Jones algorithm by seeing its robustness and presentation in real-life situations, the working face detector is robust enough to detect the face. However, the working face sensor has infrequently caused in untrue positives due to the multifaceted upbringings careful throughout the data capture. Hence, working the likelihood based method as stated in to decrease the number of untrue positives. Those wrong positives that cannot be alleviated using the method labeled in are then visually resolute and physically rectified to recover the general presentation of the scheme. Here, feature removal component procedures the developed biometric statistics and excerpts a feature set using PCA. Then the scheme associates the traits with the patterns of the demanded individuality providing at registration stage. It foodstuffs face match score by matching algorithm.

### *B. Fingerprint Matcher*

This module obtains the finger biometric data since a user and rights his individuality. Feature extraction, procedures the learned biometric statistics and excerpts a feature set using Minutiae Extractor and Orientation. Fingerprints can be confidential as weakly-order touches showing a leading ridge location at each opinion. The location field delivers a rough account of the fingerprint pattern that can be assessed with sensible correctness even from noisy input images. Here, describe the location of each minutia with admiration to the input fingerprint pattern founded on a descriptor that includes info about the direction arena in a comprehensive area around the minutia opinion. Since the point location typically exhibitions small latitudinal disparities between neighborhood pixels, a big area of the location field can be rebuilt from the orientation angles expected in a comparatively small number of sample points. The sample points allotted to each minutia can be prearranged in a round pattern around the minutia location. Then the scheme associates the characters with the patterns of the demanded individuality providing at registration phase. It harvests finger match score using matching algorithm

### *C. Secure fusion rule*

The safe score-level synthesis procedures future so distant is founded on openly demonstrating performance attacks in contradiction of every matcher

as share of the deceiver delivery. In this research, spoofing-aware score-level synthesis rubrics remain future founded on LLR rule and Fuzzy Logic. This rule comprises the prospect of trying a presentation attack in contradiction of each matcher. It estimate fake score distribution by appropriate a Gamma delivery on the consistent exercise statistics. If an attack is attempted, then consistent score follows a delivery of zero-effort impostors.

### *D. Fuzzy Logic*

The advance of a fuzzy logic scheme includes 3 central stages: (i) significant fuzzy variables and their association purposes (fuzzification procedure); (ii) generating the fuzzy instructions that define relationships among the fuzzy variables; (iii) founding a misappropriated defuzzification technique

- In the fuzzification step, each one of the inputs is modelled as a fuzzy adjustable.
- A association purpose charts every fuzzy adjustable into a real amount on the [0, 1] variety
- Selecting a suitable association purpose is critical designed for custody the language appearance expressive.
- Aimed at the height quality language appearance, chooses a min–max function
- Comparison slashes through little excellence must need little masses in the last production.

### *E. LLR*

- Spoofing-aware score-level fusion instructions remained future, by way of variations of the famous LLR regulation.
- Lease I be a double chance mutable that designates if the operator is fake (I =1) otherwise honest (I = 0).
- Evaluate the LLR among the honest delivery and the fake delivery
- Typically, the provisional deliveries are erudite by a exercise dataset w
- The similarity score will shadow a honest one.

Finally, fusion of LLR & Fuzzy logic obtains the aggregated score. The combined score is lastly associated with a threshold t to choose whether honest operator or fake.

## V. PERFORMANCE EVALUATION

The presentation of the future synthesis systems remained assessed by means of dual biometric schemes: a face gratitude scheme applied by eigenfaces then openly obtainable fingerprint scheme industrialized by NIST. The excellence of a fingerprint taster remained calculated by the NFIQ software, too established through NIST. The excellence aimed at a face image remained physically allocated founded going on the face revolution, brilliance and facial appearance. In applied request, the face image excellence might be mechanically intended. In this research, usage the subscript face and finger to mention to the resemblance score for face and fingerprint schemes, separately.

A multimodal dataset remained shaped through arbitrarily joining operators since the FVC2004-DB1 dataset. Here run the experimentations five times, existence that a novel multimodal dataset remains arbitrarily shaped on every period. The arbitrarily choose six operators after the multimodal dataset to train the fusion replicas, then custom the additional twelve operators toward track the checks.

### *A. Average Detection Error Trade-off (DET)*

These arcs explosion FRR vs FAR for all working opinions arranged a suitable alliance climbing By means of our-meta perfect, concept a domestic of DET arcs, every gotten through faking an attack situation in contradiction of a solitary matcher.

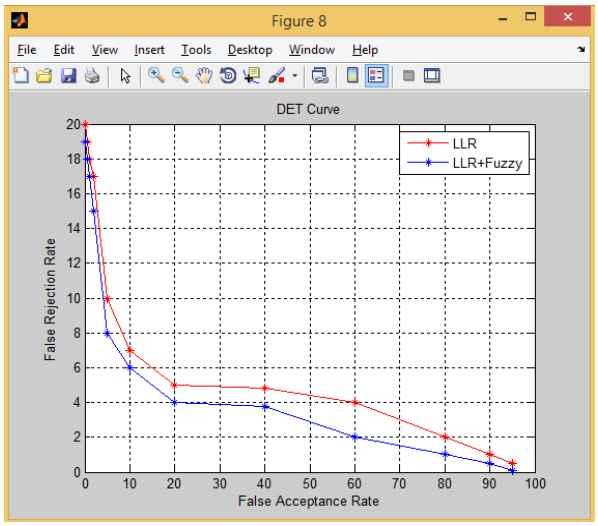


**Fig. 2. Comparison of DET curve**

To properly comprehend our assessment, recall that spoofing organizes not touch the matching notch delivery of honest operators, i.e., the FRR below attack prepares not alteration. The analysis tourist attractions LLR + Fuzzy synthesis law is extra subtle to differences popular the production of an assumed matcher. This can be renowned by likening the sureness groups consistent to attacks in contradiction of the fingerprint then the face matcher. In our situation, synthesis rubrics are usually more susceptible to attacks directing the fingerprint matcher, by way of the sureness groups consistent to fingerprint performance attacks are classically extra removed to advanced mistake rates. The aim is just that the fingerprint matcher is further exact than the face one in this situation, and, therefore, once the previous remains below attack, the matching scores of spoof deceivers and honest operators incline to overlay extra.

From the DET arcs, one might similarly note that normal procedures remain usually extra precise in the nonappearance of attack than safe synthesis rules, settling the trade-off among the presentation in the

nonappearance and in the attendance of spoofing. The Smallest is an exclusion, as it exhibitions a advanced FAR. The aim is that this law first receives the honest right if completely the joint scores are adequately tall. Therefore, to keep an satisfactory, little FRR, unique consumes toward skill for a advanced FAR, then this might too deteriorate safety against spoofing, equally to nature

## VI. CONCLUSION

In this research, I have identified that the influence of spoofing attack in multimodal biometric schemes. Our experimentations display that once consuming outdated synthesis arrangements (i.e. LLR or slanted amount), a counterfeiter container intensely intensification the probabilities of extremely a multimodal scheme through spoofing lone one of the biometrics. To decrease this softness, future binary original synthesis arrangements that take into explanation the safety of each unimodal biometric scheme. The experimentations designate the being of a compromise among appreciation correctness and heftiness in contradiction of presentation attacks. The experimentations also designate that the fuzzy synthesis system had a better general presentation when associated with the probabilistic fusion system. The upcoming, determination tool a exercise procedure to automatically optimize the connotation determinations in the fuzzy logic synthesis, and test together fusion systems with a wider variety of limitations.

## REFERENCES


[1] A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for Video Technology 14 (1) (2004).

[2] C.Sanderson, K.K. Paliwal, Identity verification using speech and face information, Digital Signal Processing 14 (2003) 449–480.

[3] J.Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, Multimodal biometric authentication using quality signals in mobile communications, in: Proceedings of the 12th International Conference on Image Analysis and Processing (ICIAP03), August 2003.

[4] J.Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, J. Bigun, Discriminative multimodal biometric authentication based on quality measures, Pattern Recognition 38 (5) (2005) 777–779.

[5] K.-A. Toh, X. Jiang, W.-Y. Yau, Exploiting global and local decisions for multimodal biometrics verification, IEEE Transactions on Signal Processing 52 (10) (2004) 3059–3072.

[6] A.Ross, A.K. Jain, Information fusion in biometrics, Pattern Recognition Letters 24 (2003). [7] Y. Wang, T. Tan, A.K. Jain, Combining face and iris biometrics for identity verification, in: Lecture Notes in Computer Science, vol. 2688, 2003, pp. 805–813.

[7] K.Nandakumar, Y. Chen, S.C. Dass, A.K. Jain, Likelihood ratio-based biometric score fusion, IEEE Transactions on Pattern Analysis and Machine Intelligence 30 (2) (2008) 342–348.

[8] S.Tulyakov, V. Govindaraju, Classifier combination types for biometric applications, in: CVPRW '06: Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop, 2006, IEEE Computer Society, Washington, DC, USA, pp. 58, ISBN: 0-7695-2646-2, doi: 10.1109/CVPRW.2006.54.

[9] E.Marasco, P. Johnson, C. Sansone, S. Schuckers, Increase the security of multibiometric systems by incorporating a spoofing detection algorithm in the fusion mechanism, in: C. Sansone, et al. (Eds.), Proceedings of the International Workshop on MCS, Lecture Notes in Computer Science, vol. 6713, Springer, Berlin, 2011, pp. 309–318, http://dx.doi.org/10.1007/978-3-642-21557-5_33

[10] I.Chingovska, A. Anjos, S. Marcel, Anti-spoofing in action: Joint operation with a verification system, in: Proceedings of the International Conference on Computer Vision and Pattern Recognition, Workshop, 2013, pp. 98–104, http:// dx.doi.org/10.1109/CVPRW.2013.22.

[11] N.Poh, R. Wong, G.-L. Marcialis, Toward an attack-sensitive tamper-resistant biometric recognition with a symmetric matcher: a fingerprint case study, in: Proceedings of the Symposium on Computational Intelligence in Biometrics and Identity Management, 2014, pp. 1–6.

[12] R.N.Rodrigues, L.L. Ling, V. Govindaraju, Robustness of multimodal biometric fusion methods against spoof attacks, J. Vis. Lang. Comput. 20 (3) (2009) 169–179

[13] Z.Akhtar, G. Fumera, G. Marcialis, F. Roli, Evaluation of serial and parallel multibiometric systems under spoofing attacks, in: Proceedings of the International Conference on Biometrics: Theory, Applications and Systems, 2012, pp. 283–288, http://dx.doi.org/10.1109/BTAS.2012.6374590

[14] E.Marasco, Y. Ding, A. Ross, Combining match scores with liveness values in a fingerprint verification system, in: Proceedings of the International Conference on Biometrics: Theory, Applications and Systems, 2012, pp. 418–425, http://dx.doi.org/10.1109/BTAS.2012.6374609

[15] G.Fumera, G. Marcialis, B. Biggio, F. Roli, S. Schuckers, Multimodal antispoofing in biometric recognition systems, in: S. Marcel, et al., (Eds.), Handbook of Biometric Anti-Spoofing, Springer, London, 2014, pp. 165–184.

[16] I.Chingovska, A. Rabello dos Anjos, S. Marcel, Biometrics evaluation under spoofing attacks, IEEE Trans. Inf. Forensics Secur. 9 (12) (2014) 2264–2276. http://dx.doi.org/10.1109/TIFS.2014.2349158

[17] A.Anjos, M.M. Chakka, S. Marcel, Motion-based counter-measures to photo attacks in face recognition, IET Biometrics 3 (3) (2013) 147–158.