ANTI-FORENSIC RESISTANT LIKELIHOOD RATIO COMPUTATION: A CASE STUDY USING FINGERPRINT BIOMETRICS

Norman Poh, Nik Suki, Aamo Iorliam and Anthony TS Ho

Department of Computing, University of Surrey
Guildford, GU2 7XH, Surrey, UK

ABSTRACT

One of the major utilities of biometrics in the context of crime scene investigation is to identify people. However, in the most sophisticated cases, criminals may introduce the biometric samples of innocent individuals in order to evade their own identities as well as to incriminate the innocent individuals. To date, even a minute suspect of an anti-forensic threat can potentially jeopardize any forensic investigation to the point that a potentially vital piece of evidence suddenly becomes powerless in the court of law. In order to remedy this situation, we propose an anti-forensic resistant likelihood ratio computation that renders the strength of evidence to a level that is proportional to the trustworthiness of the trace, such that a highly credible evidence will bear its full strength of evidence whilst a highly suspicious trace can have its strength of evidence reduced to naught. Using simulation as well as a spoof fingerprint database, we show that the existing likelihood ratio computation is extremely vulnerable to an anti-forensic threat whereas our proposed computation is robust to it, thereby striking the balance between the utility and threat of a trace.

Index Terms— Anti-forensic, likelihood ratios, tampered images, trustworthiness, strength of evidence

1. INTRODUCTION

1.1. Motivation

The trustworthiness of biometric evidence is a major concern when presenting such evidence in court. As a forensic practitioner, the assessment of likelihood ratio (LR) is the most genuine means to evaluate biometric trace [1]. Anti-forensic techniques are recently so rampant to alter biometric trace that this becomes a great concern to the forensic and biometric communities. Digital tampering and sensor tampering are the two main ways used by anti-forensic practitioners. Even though the LR approach statistically estimates the value of a biometric sample, performing a LR on a digitally tampered or spoofed biometric sample will pose a threat to innocent people.

In order to reduce the threat posed by the aforementioned anti-forensic issues, we are motivated to develop a framework that determines the strength of the evidence and also show if such a biometric sample is worth presenting as evidence in court or not.

1.2. Strength of Evidence

Meuwly and Veldhuis [2] proposed that forensic strength of evidence statements should preferably be likelihood ratios calculated using relevant data, quantitative measurements and statistical models in order to overcome the inconclusive category of evidence outcome. The calculated results may later be supported by an expert’s opinion if needed. This is to ensure that one can use and evaluate all possible evidence collected and present it in court. A large body of literature [3–9] asserts that likelihood ratio computation is a reliable, scientifically validated, and approved method for evaluating forensic biometric trace.

Validity and reliability are two virtues that cannot be overly emphasized in forensic science. Morrison et al. [10] addressed that one should be able to present the accuracy of their output results together with how precise their approach could be. It will be misleading to court if forensic practitioners only report the latter result without giving a statement concerning the reliability of their result. At the end, it is the judge who has the ultimate power to admit or reject the presented evidence based on investigator’s testimony [11].

The main concern in this paper is that if the trace collected from a crime scene is not original or has been tampered with in any way, evaluating the calculated result from a trusted likelihood ratio framework could be jeopardised. By taking into consideration the importance of knowing the trustworthiness of the evidence, we propose an anti-forensic methodology that can take into account the trustworthiness of piece of biometric trace. The context of trustworthiness in this paper, we refers to the ability to place trust on the collected trace and being assured that the trust shall not be betrayed. Latter we implement it in the usual likelihood ratio computation framework, thereby striking the balance between the utility and threat of a trace proportionately to its level of trustworthiness.

1.3. Questionable Images as Evidence

In general, there are two types of tampered images: (i) digital tampering; and (ii) spoofed samples. Taking into consideration of a biometric sample, digital tampering refers to a process where a trace image is maliciously tampered with in order to be presented as evidence in the court or to tarnish someones...
Technique. Intuitively, the anti-forensic resistance LLR should represent the defence hypothesis whereas \( H_0 \) represents the null hypothesis. Put differently, \( H_0 \) represents the prosecution hypothesis whereas \( H_1 \) represents the defence hypothesis.

However, the log-likelihood term, \( LLR(E) \) has no mechanism that considers the trustworthiness of the evidence. If the evidence has been tampered with, then, we would like the \( LLR(E) \) term to reduce to zero so that it does not carry any strength any more. On the other hand, if the \( LLR(E) \) is trustworthy, we shall keep \( LLR(E) \) to assume its original value. In other words, we need a trustworthy log-likelihood ratio, just in case our evidence has been tampered with by an anti-forensic technique. Intuitively, the anti-forensic resistance LLR should be of the form of:

\[
LLR_{\text{resist}}(E) \approx w \log \frac{p(E|H_0)}{p(E|H_1)}
\]

(1)

where \( w \in [0, 1] \).

We describe a procedure that can achieve this. Let \( P(T = 1|t) \) be the probability of the trustworthiness \( T \) of the sample given the measurement of potential tampering, \( t \) which is usually a feature vector. In the case of a digital image, \( t \) is deviation from the Benford’s law, which is a probability distribution that has been widely used to detect tampering in financial data [17]; and has recently been used to detect digital tampering of fingerprint images [18]. The feature vector \( t \) can also characterise the liveness of a biometric sample, e.g., local binary patterns (LBP) [19], so that \( P(T = 1|t) \) can be interpreted as the probability of a sample being taken from a live finger rather than spoof materials. In any case, we recognise that the probability of trustworthiness, \( P(T = 1|t) \), is a function of the tampering measure, \( t \); hence, this can be written as \( w(t) \in [0, 1] \).

A tamper-resistant likelihood can then be defined as:

\[
p(E|H_k, T = 1, t) = \frac{1}{Z_k(w(t))} p(E|H_k)^{w(t)}
\]

(2)

for both prosecution and defence hypotheses, \( k \in \{0, 1\} \), where \( Z_k(w(t)) \) ensures that the left hand side term is properly normalized, i.e., \( Z_k(w(t)) = \int_{k} p(E|H_k)^{w(t)} \), noting that this term is a function of the probability of trustworthiness term, \( w(t) \), but not of the evidence, \( E \), itself since it is integrated out of the equation.

Using the likelihood ratio framework, the tamper-resistant LLR can consequently be written as:

\[
LLR_{\text{resist}}(E) = \log \frac{p(E|H_0, T = 1, t)}{p(E|H_1, T = 1, t)} = \log \left( \frac{(Z_0(w(t)))^{-1} p(E|H_0)^{w(t)}}{(Z_1(w(t)))^{-1} p(E|H_1)^{w(t)}} \right)
\]

(3)

\[
= w(t) \log \frac{p(E|H_0)}{p(E|H_1)} - \log \frac{Z_0(w(t))}{Z_1(w(t))}
\]

where in (3), we have plugged in the tamper-resistant likelihood term as defined in (2). By rewriting the equation as a function of the conventional \( LLR(E) \), we observe that the tamper-resistant LLR is made up of two terms, i.e., an evidence-based log-ratio term and a normalizing log-ratio term that is independent of the evidence. While the first term rescales the conventional \( LLR(E) \) by \( w(t) \), the second term, \( \epsilon(w(t)) \equiv - \log Z_{\text{resist}}(w(t)) \), introduces the bias required in order to achieve equality. In practice, the second term tends to cancel out each other, causing it to assume a significantly small value that is close to zero, i.e., \( \epsilon(w(t)) \approx 0 \). Put differently, the absolute value evidence-dependent term is many orders larger than that of the normalizing term:

\[
\log \left( \frac{p(E|H_0)}{p(E|H_1)} \right)^{w(t)} \gg \log \frac{Z_0(w(t))}{Z_1(w(t))}
\]

Following this rationale, by dropping \( \epsilon(w(t)) \), we obtain the intuition as specified by (1). Despite being a less important
term, it should not be neglected because the absolute value of LLR is often used to interpret the strength of a piece of evidence. In summary, although we started with an intuition, by using probability axioms, we have derived a tamper-resistant LLR that is a shifted and scaled version of the conventional LLR, thus introducing minimal modification to a widely accepted practice. Since the modification is easy to understand, it is more likely to be accepted and adopted.

2.1. Assessing the Probability of Trustworthiness using the Bayes Theorem

The key to obtaining a resistant-tampering likelihood ratio is to evaluate \( w(t) = P(T = 1|t) \). This term can be calculated using the Bayes theorem [20] or through a discriminant function such as logistic regression that gives probabilistic output. Here, we shall present the first method; and the readers are referred to [20] for the second method.

From the Bayes theorem, the probability of Trustworthiness is given by:

\[
P(T = 1|t) = \frac{P(T)p(t|T = 1)}{\sum_{T' \in \{0,1\}} P(T')p(t|T')}
\]

where \( p(t|T) \) is the likelihood of evidence of tampering given that its state of tampering, \( T \), which can be either true or false. This is because a sample has either been tampered with or it has not. \( P(T) \) is the prior probability of tampering. Importantly, \( p(t|T) \) is obtained from a training database of tampered and untampered samples whereas the prior \( P(T) \) is manually set for each and every case work.

The value of \( P(T) \) depends on a number of factors. When solving a case work, if there is a reason to be believe that anti-forensic could have taken place, then, it is sensible to set the prior probability of tampering \( P(T) \) appropriately. On the other hand, if an evidence is considered 100% trustworthy, one can simply set \( P(T) = 1 \) so that the tamper-resistant LLR is exactly the same as the conventional LLR \( E \). In summary, \( P(T) \) offers a flexible way of specifying trustworthiness that reflects an investigator’s belief. This mechanism effectively renders the conventional LLR resistant to antiforensic attempts.

2.2. Analysis of the weighted LLR

Let us now analyse the range of values assumed by a tamper-resistant LLR as in (4). For this purpose, we shall focus on the evidence-dependent log-ratio term and drop the log-ratio normalizing term (which a very small value).

\[
LLR_{\text{resist}}(E) \approx w(t) \log \frac{p(E|H_0)}{p(E|H_1)}
\]

If the normal \( LLR(E) \) is bounded in \([-b, b]\), the tamper-resistant LLR will be bounded in \([-bw(t), bw(t)]\). Since \( w(t) \) takes a value between zero and one, the tamper-resistant LLR will be at most as large as \([-b, b]\) but as small as 0. Therefore, \( w(t) \) directly controls the strength of evidence.

We now illustrate this with an example. We first plot the likelihood of evidence given \( H_k, p(E|H_k) \), where the evidence is a matching score, for the prosecution hypothesis \( H_0 \) (\( k = 0 \)); as well as the defence hypothesis \( H_1 \) (\( k = 1 \)). Because the likelihoods have been modelled on original, non-tampered data, we are really estimating \( p(E|H_k, T = 1) \) to write more explicitly. Figure 1 plots the pair of likelihood controlled by \( w \) which is set to different values between zero and one.

![Figure 1: A demonstration of likelihoods \( p(E|H_k, T = 1) \) for \( k \in \{0, 1\} \) with different weightings of \( w \in \{1, 0.9, 0.75, 0.5, 0.25, 0.1\} \) from the thinnest to the thickest lines.](image)

In addition, with decreasing \( w \), the likelihoods \( \frac{1}{p(E|H_k|T = 1)}w \) for both classes, \( k \in \{0, 1\} \) also become smaller and smaller. This should lead to smaller strength of evidence in terms of log-likelihood ratio. In the experimental section, we will let \( w \) to be controlled by the probability of a live, non-tampered sample.

3. EXPERIMENTS

3.1. Database

In order to study the potential effect of tampering, we have chosen to use a biometric database containing spoof samples. This enables us quantify objective how strong the proposed anti-forensic resistant framework can withstand tampering. Specifically, we wish to examine whether or not the strength of evidence for tampered biometric samples can be reduced by our proposed method with respect to the conventional method of likelihood ratio computation.

To this end, we have chosen to use the LivDet 2011 [15] database. An interesting aspect of this database is that it contains live fingerprint images of different quality levels as well as fake fingerprint images due to the use of different fabrication materials.

In addition, with the database, we can also measure the strength of evidence under zero-effort non-match comparison which is essential to estimate \( p(E|H_1, T = 0) \).

The LivDET 2011 database contains 8000 samples. The most important key statistics relevant for our experiments are:

- 144 unique fingers containing both live and spoof samples
• 256 unique fingers containing only live samples
• 4000 fingerprints acquired using the Biometrika sensor, and another 4000 acquired using the Itadata sensor.
• 800 fake fingerprint samples for each of the five fabrication materials

We prepared the data by making an exhaustive pair-wise comparison of all the available 8,000 samples. For each of the 8,000 samples, we also estimated their liveness measure based on the Local Binary Patterns (LBP) features as described in [19]. The LBP features have been shown to outperform other competing liveness measures based on pores detection, Curvelet, Power spectrum, Wavelet energy signature evaluated on the LivDet 2011 fingerprint database. We modelled the probability of liveness given the LBP features using logistic regression [20].

The data set is divided into two equal partitions, namely a training set and a test set. The training set is used for estimating any model parameters. In this case, the models are \( p(E|H_k) \) for both \( k = \{0, 1\} \), and also \( w(t) \equiv 0 \) for all the live samples and \( w(T = 1) = 0.2 \) for the spoof samples made with any of the five fabrication materials. We also conducted a third set of experiments which is called the “oracle” where we set \( P(T = 1) = 0 \) for all the live samples and \( P(T = 1) = 1 \) for the spoof samples. This enables us to see the best possible that can be possibly achieved. The results are shown in Figure 2(d).

In the second set of experiments as shown in Figure 2(c), we created an additional simulation where we allow the investigator to weigh in his/her opinion in order to question the validity of the evidence’s trustworthiness. Therefore, rather than relying on a fully automatic liveness detector, the investigator is allowed to introduce a prior of \( P(T = 1) \) to some values. In this case, we set \( P(T = 1) = 0.8 \) for all the live samples and \( P(T = 1) = 0.2 \) for the spoof samples made with any of the five fabrication materials. We also conducted a third set of experiments which is called the “oracle” where we set \( P(T = 1) = 1 \) for all the live samples and \( P(T = 1) = 0 \) for the spoof samples. This enables us to see the best possible that can be possibly achieved. The results are shown in Figure 2(d).

As can be observed, the interquartile range of the spoofed material with the expert’s opinion become much more narrower in Figure 2(c). This shows that when the investigator exerts his/her opinion of trustworthiness to the proposed anti-forensic LLR, a much more accurate decision can be attained. Of course, if the opinion of the investigator turns out to be wrong, such an exercise will be counter productive, but can still do no worse than the conventional LLR.

The above experiments demonstrates the ability of the proposed anti-forensic computation to use the expert’s opinion in weighting the uncertainty of the evidence’s origin as discussed in Section 2.1. Furthermore, with the availability of additional prior knowledge about the integrity of the evidence (as represented by \( P(T) \)), the resultant strength of evidence is significantly reduced to a non-threatening level.
4. CONCLUSION

In this paper, we proposed an anti-forensic-resistant likelihood ratio computation that explicitly considers the trustworthiness of the evidence. We showed that the strength of evidence can be reduced to a non-threatening level when the evidence has been tampered with. Our empirical investigation shows that the strength of evidence due to spoofing can be significantly reduced in terms of the interquartile range of LLR, leaving the LLR of untampered samples, both for the match and non-match comparisons, to be roughly the same. The method can thus seamlessly be integrated with the widely accepted likelihood ratio computation without significantly modification. The proposed anti-forensic resistant computation also allows the expert’s opinion to weigh in his prior belief about the trustworthiness of a piece of evidence by simply setting the prior of \( P(T = 1) \). Possible future research directions include: (1) applying the proposed anti-forensic resistant computation to different biometric modalities; (2) investigating the effect of the proposed computation for digital tampered images; and (3) investigating the impact of various settings for \( P(T = 1) \).

5. ACKNOWLEDGEMENTS

Dr Poh received funding from the BEAT project (grant no. 284989) to carry out this work. Nik Suki would like to acknowledge Universiti Malaysia Pahang (UMP), Malaysia for the sponsorship on her PhD study. Aamo Iorliam also would like to acknowledge the financial support of Benue State University, Makurdi, Nigeria for the sponsorship of his PhD scholarship. The authors thank Prof Raymond Veldhuis for a fruitful discussion.

REFERENCES


