Recital of Poles Apart Ridge Cipher with Din

Pughazendi.N
Faculty, Department of M.C.A,
Panimalar Engineering College, Chennai.
pughazendi@yahoo.com

R.Sankar
PG Scholar, Department of M.C.A,
Panimalar Engineering College, Chennai.
cuosankar@gmail.com

Abstract— **The effect of the din distribution on the error probability of the detection test is studied here that when a class of randomly rotated spherical Ridges is used. The detection test is performed by a focused correlation detector, and the spherical codes studied here form a randomized orthogonal constellation. The colluders create a din-free forgery by uniform averaging of their individual copies, and then add a din sequence to form the actual forgery. We derive the din distribution that maximizes the error probability of the detector under average and almost-sure distortion constraints. Moreover, we characterize the din distribution that minimizes the decoder's error exponent under a large-deviations distortion constraint. Our Ridges form a randomized orthogonal code, where the randomization parameters are a rotation. The dinless forgery is obtained by uniform linear averaging of he colluders copies. The detector has access to the host signal and performs a binary hypothesis test to verify whether a user of interest is colluding.**

I. INTRODUCTION

THE Internet has drastically changed our daily lives—specifically in terms of convenient access, storage, and transmission of digital data. At the same time, this ease of access has resulted in an increase in unauthorized use. As a result, music and film industries lose millions of dollars per year. Digital ridging is one of the digital rights management techniques developed to combat copyright infringement. Digital ridges deter illegal redistribution of digital content by providing each user with their own individually marked copy of the content. While these unique marks make it possible to trace an illegal copy to a traitor, they also enable a host of nefarious assault, called *collusion assaults*. A collusion assault refers to a strategy under which a group of users forge an illegal copy from their individualized legitimate copies. Furthermore, the colluders may corrupt their forged copy by adding din, which makes the task of the ridge identifier will be harder.

For Ridges and signals defined over Euclidean spaces, the worst collusion channel subject to mean-squared distortion constraints was identified in the capacity analysis. The worst channel was the uniform linear averaging attack followed by scaling and addition of additive white Gaussian din. However, In the Ridgeing literature, the usual assumption has been that the colluders add white Gaussian din to a *dinless forgery* which they create by combining ("averaging") their signals in a linear or nonlinear fashion. Under the fixed correlation identifier, that the uniform linear averaging strategy is the most damaging one in an error-probability sense.

The randomization parameter is a rotation. Three types of constraints are considered for the assaulter's din:
1) average-distortion constraint;
2) almost-sure (a.s.) distortion constraint;
3) large-deviations constraint.
For all three versions of the problem, we derive the worst din and obtain a tight asymptotic expression for the worst-case detection error probability.

The symbol E to denote mathematical expectation and SO(N) the group of rotations on the N-sphere, and by ν_{unif} the uniform probability measure over SO(N).

II. PROPOSED SYSTEM

We derive the din distribution that maximizes the error probability of the identifier under average and almost-sure distortion constraints. Moreover, we characterize the din distribution that minimizes the identifier's error exponent under a large-deviations distortion constraint.

III. PROBLEM STATEMENT

This section defines the mathematical setup of the problem.

A. Ridge entrenching

The host signal is a sequence S = (S(1),…,S(n)) in R^N, viewed as deterministic but unknown to the colluders. Ridges are added to S, and marked copies of the signal are distributed among M users. Specifically, user m is assigned a marked copy

$$X_m = S+Q_m, \qquad m \in \{1\ldots M\}$$

where the Ridge $Q_m = \{Q_m(1),\ldots,Q_m(N)\} \in R^N$ Fig. 1 depicts the Ridge *entrenching* and the assault sculpts. The M length-N Ridges form an (N,M) Ridgeing code c = $\{Q_m, 1\le m\le M\}$. All codes considered are of *randomly rotated spherical Ridges.* First a *deterministic prototype* spherical code C_0 is designed. Here, we consider the prototype C_0 to be either an orthogonal, or a regular simplex code. The Ridge entrencher draws a random variable g uniformly distributed over SO(N) and rotates the prototype constellation C_0 by g . While C_0 is publicly known, g is a secret shared with the detector. Therefore, even though the attackers know C_0, they do not know their individual Ridges. This is a randomized Ridgeing code. The Ridges are obtained as $Q_m = \sqrt{N D_f} P_m$ and so

$$\|X_m - S\|^2 = \| Q_m \| = ND_f, \text{ for all m.} \qquad \rightarrow (1)$$

where D_f is the energy per sample for each Q_m.

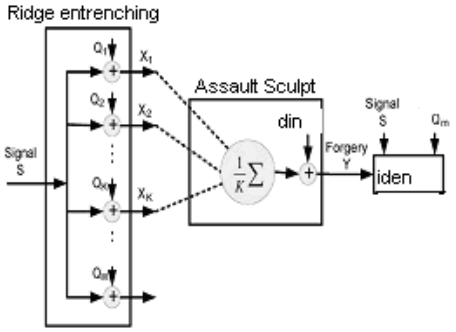

Fig. 1. Ridging process, assault sculpts, and identifier focused on user m.

B. Assault Sculpt

The assault sculpt is modeled as the uniform average of the colluders' marked signals, followed by addition of a din sequence E

$$\mathbf{Y} = \frac{1}{\mathcal{K}} \sum_{m\in\mathcal{K}} \mathbf{X}_m + \mathbf{E} = \mathbf{S} + \frac{1}{|\mathcal{K}|} \sum_{m\in\mathcal{K}} \mathbf{Q}_m + \mathbf{E} \qquad \rightarrow (2)$$

where $\mathcal{K} \subseteq \{1,\ldots,M\}$, the *coalition*, is the index set of the colluding users. We denote the size of coalition by K. The din sequence E is drawn independently $\{X_m, m \in K\}$ of from a probability distribution function (pdf) p_E with zero mean. Therefore, the assault is completely defined by the pair $\{K, p_E\}$.

The mean-squared distortion of the forgery Y relative to the host signal S is given by

$$E\|Y-S\|^2 = ND_c. \qquad \rightarrow \quad (3)$$

Here, we fix a din strength parameter and consider three types of constraints on the attackers din

1) average-distortion constraint: $E[\|E\|^2] \le N\sigma^2$;
2)almost-sure distortion constraint are given as $\Pr[\|E\|^2] > N\sigma^2] = 0$;
3) large-deviations constraint are given as $\Pr[\|E\|^2] > N\sigma^2] \le e^{-N\lambda}$ for some $\lambda \ge 0$.

C. alert association identifier

The identifier knows neither the number of colluders K nor the din pdf p_E. It has access to the host signal S (nonblind detection) and subtracts it from the forgery Y to form the centered data Y - S.

Ideally the detector must return the list of all colluders. However, this task proves to be too hard. Instead we introduce a detector structure that aims at determining whether a certain user's mark is present in the forgery Y. it will be called as identifier *focused*, because it decides whether a particular user of interest is a colluder. Given that Ridging schemes are used as deterrents against illegal redistribution, catching one member of the coalition is often sufficient for this purpose.

The focused identifier performs a binary hypothesis test that returns a guilty or not guilty verdict for the user it is focused on.

D. Bayesian Error Probability

For a given coalition K, attack A, and detection rule Q_m, a natural cost function for the detector focused on user m is the error probability

$$P_e(m,K,p_E) \triangleq \lambda P_I(m,K,p_E) + (1-\lambda) P_{II}(m,K,p_E). \qquad \rightarrow (4)$$

where $\lambda \in [0,1]$. The expression (4) corresponds to a Bayes risk. Moreover, minmax and Neyman–Pearson hypothesis testing correspond to a Bayes hypothesis testing for a certain choice of λ. we view the error probability as a function of the number of colluders K and the din distribution p_E.

Another simplification that arises for large N is that the influence of the priors vanishes. Thus, for convenience, it will be

consider equal priors. The Bayesian cost function (4) for the focused detector is then expressed as

$$P_e(K, p_{\mathbf{E}}) \triangleq \frac{1}{2} P_{\mathrm{I}}(K, p_{\mathbf{E}}) + \frac{1}{2} P_{\mathrm{II}}(K, p_{\mathbf{E}}) \quad \rightarrow \quad (5)$$

where P_I and P_{II} denote the error probabilities for the focused detector.

The corresponding error probability is denoted as the feasible set for p_E depends on the constraint used. For fixed K and a sequence of orthogonal Ridges and din distributions indexed by N, we also define the error exponent corresponding to the worst-case din distribution as

$$e^*(K) \triangleq -\limsup_{N \to \infty} \frac{1}{N} \ln \sup_{p_{\mathbf{E}}} P_e(K, p_{\mathbf{E}}), \quad \rightarrow \quad (6)$$

IV. RADIAL DIN

We assume a randomly rotated spherical Ridge constellation and the average assault for the coalition to prove the best strategy for the Ridge entrenching is to rotate the Ridge constellation uniformly on the-sphere.Consider the following strategies for the Ridge entrencher and the colluders:

1) The Ridge entrencher selects a probability measure on the rotation group SO(N). The value of g is a secret shared with the identifier.

2) The colluders select a probability measure νc on SO(N) and their din vector be E=g'E'. Hence E follows the rotation-averaged distribution.

V. WORST-CASE DIN

A. Worst-Case Din Under Average-Distortion Constraint.

Denote the set of all din pdfs satisfying the average-distortion constraint. Conditioned on R = r and given the threshold ι, the decision boundary Ω cuts a spherical cap away from the N-dimensional sphere of radius R=r. Fig. 2 shows the decision boundary and the corresponding spherical cap. The half angle corresponding to the spherical cap is denoted by θ.

The error probability, conditioned on R=r, is the normalized volume of the shaded spherical cap.

B. Worst-Case Din Under Almost-Sure Distortion Constraint

Under the almost-sure distortion, the support of P_R is given by

$$\mathrm{Supp}[p_R] = [0, \sqrt{N\sigma^2}].$$

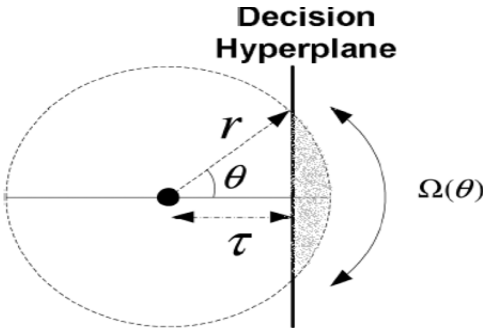

Fig. 2. Decision threshold ι and norm r of din vector E.

As was to be expected, the colluders can maximize the error probability of the identifier by concentrating their din power at the maximum radius allowed by the almost-sure constraint.

C. Worst-Case Din Under Large-Deviations Constraint

We know that the colluders can launch a nefarious assault when they choose impulsive din. This was allowed because the assaulters are only limited by the *average* distortion constraint. The probability of a large distortion vector E is given by $A = O(K^2/N)$ and is thus fairly significant. The din pdf design problem when the assaulters are subject to the additional large-deviations constraint on the magnitude of the din vector. For any $\lambda > 0$ we may thus say that Gaussian din is essentially the worst din, for K large enough.

VI. CONCLUSION

We first characterized the worst-case noise under an average-noise power constraint. Under the average-distortion model, the colluders are able to dramatically affect detector performance but at the expense of introducing a huge mean-squared distortion in their forgery. Here the colluders exploit a critical vulnerability of the system, that is, it was optimized relative to the mean-squared error criterion and not a perceptual criterion. Under the almost-sure distortion model, the colluders are absolutely precluded from introducing any large mean squared error distortion. This is particularly interesting because this attack has been widely assumed in multimedia fingerprinting practice, and so our results show that it is a good choice for the attackers. These performance fingerprints are drawn from a regular simplex prototype.

REFERENCES

[1] N. Kiyavash, P. Moulin, and T. Kalker, "Regular simplex fingerprints and their optimality properties," IEEE Trans. Inf. Forensics Security 10.1109/TIFS.2009.2025855.
[2] P. Moulin and J. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 563–593,
Mar. 2003.
[3] A. Somekh-Baruch and N. Merhav, "Achievable error exponents for the private fingerprinting games," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1827–1838, May 2007.
[4] Y. Wang and P. Moulin, "Capacity and random-coding error exponent for public fingerprinting game," in *IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006.
[5] P. Moulin, "Universal fingerprinting:
Capacity and random-coding exponents,"
IEEE Trans. Inf. Theory, Available from arxiv: 0801.3837v2 [cs.IT], submitted for publication.
[6] Y. Wang and P. Moulin, "Capacity and optimal collusion attack channels for Gaussian fingerprinting games," in *Proc. IS&T/SPIE Sym.*
Electronic Imaging–Conf. Security, Steganography, and Watermarking Multimedia Content IX, San Jose, Jan. 2007.
[7] P. Moulin, "Optimal Gaussian fingerprint decoders," in *IEEE Conf. Acoustics, Speech and Signal Processing (ICASSP)*, Taipei, Taiwan,
2009.
[8] I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum Watermarking for images, audio, and video," in *IEEE Int. Conf. Image Processing (ICIP)*, 1996, pp. 243–246.
[9] H. S. Stone, Analysis of Attacks on Image Watermarks With Randomized Coefficients NEC Research Institute, Tech. Rep. 96-045, 1996.
[10] Z. Wang, M. Wu, H. Zhao, W. Trappe, and K. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal Modulation, "*IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 804–821, 2005.
[11]http://www.gotdotnet.com/track_details/ tracks. Asp
[12]http://www.networkcomputing.com/ datavault.asp
[13]http://www.dotnet247/247reference/ default.aspx
[14]http://www.sourcefordge.com/technology/
tutorial_default.aspx

AUTHORS PROFILE

N.Pughazendi is presently working as a Faculty, Master of Computer Application at Panimalar Engineering College, Chennai. He is Pursuing his Doctoral Program in Manonmaniam Sundaranar University. He has 8 years teaching experience. He has attended more than 22 Faculty Development Programs in and around India. He has presented research papers in more than 6 national and international conferences. His research areas include Data mining and Network security.

R.Sankar is PG Scholar, M.C.A Department in Panimalar Engineering College. He had presented 3 papers in National symposium.