International Journal of Information Technology and Knowledge Management
July-December 2012, Volume 5, No. 2, pp. 239-243

CONFECTION OF FUZZIFIED UNCERTAINTY AND RANDOMNESS TOWARDS DECEPTION DETECTION IN VIDEO YAKKING USING ANSCHLUSS TECHNIQUES

S. Rajkumar*

Abstract: The development of computer science field not only enriches the knowledge but also provides few possibilities for spoiling the societal communication values. The recent mode of Computer communication enables sophisticated techniques for communication and disables few features for safe video yakking process to ensure the protection of our belongings. Fake video chatting is the recent technique in the fraudulent mode of communication strategies. Only expertise knowledge people are the exceptional to secure themselves in these intelligent attacks .Manual or casual handling of deception detection in the case of Fake Video Yakking is a tedious process to provide maximum security. In this research paper we provide the techniques of Randomized approach, Fuzzified approach and Uncertainty approach with its individual and combined implementation strategies. We perform the efficiency comparison among these three techniques including all such combinations with an experiment. The results are compared and discussed for future developments.

Keywords: Deception, Detection, Uncertainty, Randomness, Fuzziness

1. INTRODUCTION

Detection of Deception is useful for everyone in our society in order to use in everyday situations where telling the truth from a lie can help prevent you from being a victim of fraud/ scams and other deceptions. This is just a basic run down of physical gestures and verbal cues that may indicate someone is being a distrust person [1].

1.1 Fuzzification

Fuzzy sets have movable boundaries, *i.e.*, the elements of such sets not only represent true or false values but also represent the degree of truth or degree of falseness for each input [2].

Fuzzy logic is the part of artificial intelligence or machine learning which interprets a human's actions. Computers can interpret only true or false values but a human being can reason the degree of truth or degree of falseness. Fuzzy models interpret the human actions and are also called intelligent systems.

1.2 Randomness

The Oxford English Dictionary defines 'random' as "Having no definite aim or purpose; not sent or guided in a particular direction; made, done, occurring, etc., without method or conscious choice; haphazard". This concept of randomness suggests a non-order or non-coherence in a sequence of symbols or steps, such that there is no intelligible pattern or combination [4].

* Bharathiar University, NIET, Coimbatore, India, *E-mail: rajkumar_proff@rediffmail.com*

C. Randomized Algorithm

A randomized algorithm is an algorithm which employs a degree of randomness as part of its logic. The algorithm typically uses uniformly random bits as an auxiliary input to guide its behavior, in the hope of achieving good performance in the "average case" over all possible choices of random bits. Formally, the algorithm's performance will be a random variable determined by the random bits; thus either the running time, or the output (or both) are random variables.

1.4 Uncertainty

Uncertainty represents Decision making, the situation where the current state of knowledge is such that, the order or nature of things is unknown, the consequences, extent, or magnitude of circumstances, conditions, or event is unpredictable and credible probabilities to possible outcomes cannot be assigned.

2. PROPOSED RESEARCH MODEL

The following diagram illustrates the implementation of Randomized approach, Fuzzy logic and Uncertainty in the deceptive datum with three different nodal sectors. Primary direction focuses on individual implementation of Randomness, Uncertainty and Fuzzy logic, Secondary direction focuses on dual implementation of Random Uncertainty, Fuzzy Uncertainty and Random Fuzzy and the final direction focuses on the combined implementation of Randomness, Fuzziness and Uncertainty.

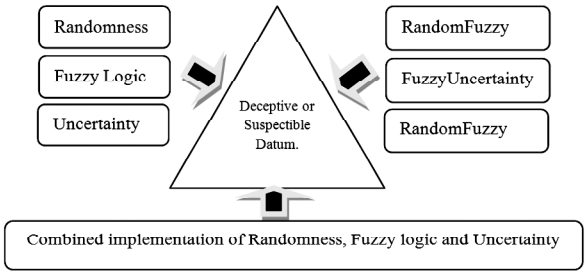

Figure 1: Proposed Model

3. RESEARCH METHODOLOGY

Consider the Deception Detection Factor as D_f, the value of D_f is surrounded by the implementation effects of Randomness, Fuzzy and Uncertainty with individual or combined application.

$r(X)$-Represents Randomized calculation for Datum-X.

$f(X)$-Represents Fuzzified calculation for Datum-X.

$u(X)$-Represents Uncertainty calculation for Datum-X.

R - Randomized evaluation of Datum-X.

F - Fuzzified evaluation of Datum-X.

U - Uncertainty Evaluation of Datum-X.

RF - Randomized and Fuzzified evaluation of Datum-X.

FU - Fuzzified & Uncertainty evaluation of Datum-X.

RU - Randomized & Uncertainty evaluation of Datum-X.

RFU - Randomized, Fuzzified and Uncertainty evaluation of Datum-X.

D_f(=1/2*(Max(R,F,U,RF,FU,RU,RFU) + MAX(IaI, IbI, c, d, e, x, y)) such that

$R = (1-a)*r(X)$ or $IaI * r(X)$, if $a > 0$ or $a<0$ respectively.

$F = (1-b)*(f(X)$ or $IbI * f(X)$, if $b>0$ or $b<0$ respectively.

$U=c*u(X)$

RF=Max(R, F) + d.

FU=Max (F, U) + e.

RU=Max(R, U) + x.

RFU=Max(R, F, U, RF, FU, RU) + y.

Where a, b, c, d, e, x, and y is Real numbers and lies between 0 &1.

a = No of Logical Factors-No of Non-Logical Factors / Total No of Factors.

b= No of Relational Categories-No of Non-Relational Categories / Total No of Categories.

c=No of suspected Occurrences/Total No of Occurrences.

$d = (IaI + IbI)/10$.

$e = (IbI + IcI)/10$

$x = (IcI + IaI)/10$

$y = (IaI + IbI + c + d + e + x)/10$.

3.1 Randomized Approach $r(X)$ Computation

1. Age/Sex/Location Suspect- $a1(X) = 0.1$
2. Users wall titled "Enable Video Calls" – $a2(X) = 0.2$
3. Invite people through message "Video Calling: Talk to your friends face-face"–$a3(X) = 0.3$
4. Voice Resemblance & Synchronization – $a4(X) = 0.4$
5. Invalid Profile – $a5(X) = 0.5$
6. Irrelevant Content 5 $a6(X) = 0.6$
7. Different or unusual appearance- $a7(X) = 0.7$
8. Non supporting Site rating by browsers- $a8(X) = 0.8$
9. Grainy/Choppy video- $a9(X) = 0.9$
10. Processed with wrong credentials- $a10(X) = 1.0$

(Purposive faultiness)

$$R(X) = \sum_{I=1}^{10} a_i(X)/10$$

3.2 Fuzzified Approach $f(X)$ Computation

1. Looping ($f_i(X) = 0.9$)
2. Invalid-whois executable result. ($f_i(X) = 0.8$)
3. Abnormal Conversation content. ($f_i(X) = 0.7$)
4. Inappropriate Conversation frequency ($f_i(X) = 0.6$)
5. Collect basic profile information ($f_i(X) = 0.5$)
6. Popping up a dialogue box ($f_i(X) = 0.4$)
7. Website forgery ($f_i(X) = 0.99$)
8. 3rd party application-(Eg: Camersoft webcam) ($f_i(X) = 0.1$)
9. Inaccurate Lip synchronization ($f_i(X) = 0.2$)
10. Forceful reconnection request for purposive termination from receiver side. ($f_i(X) = 0.3$)

$$F(X) = \sum_{I=1}^{10} f_i(X)/10$$

3.3 Uncertainty Evaluation $u(X)$ Computation

GUM (Guide to the Expression of Uncertainty in

Measurement) approach is that it is not possible to state how well the true value of the measurand is known, but only how well it is believed to be known.

1. Genuine Source: Belief/Disbelief 0.1
2. Genuine IP Address: Belief/DisBelief 0.2
3. Black Bars on Video Edges:: Belief/DisBelief 0.3
4. Text Over Video: Belief/DisBelief 0.4
5. Hands Not Typing: Belief/DisBelief 0.5
6. Genuine Alert/Warning: Belief/Disbelief 0.6
7. Not Blacklisted: Belief/Disbelief 0.7
8. Video jump in requested action: Belief/Disbelief 0.8
9. Forced Age/Sex/Loc Request: Belief/Disbelief 0.9
10. Known user Response: Belief/Disbelief 0.99

$$u(X) = \sum_{I=1}^{10} u_i(X)/10$$

4. EXPERIMENT

While Googling with the video chat options we are facing a lot of video chat servers in this day today's life. The options are as follows,

1. EkkoTV
2. RandomDorm
3. StreamFame
4. ChatRide
5. Imo.im
6. MeBeam
7. BoostCam
8. Confabio
9. WooMe
10. Chatroulette
11. TinyChat
12. 6rounds

Some other familier websites/Mail servers/Social networks for video chat are as follows,

1. Gmail.
2. Yahoo messenger
3. Facebook.
4. MSN services
5. Skype
6. Twitter.
7. Tiny chat.
8. Orange. etc

Let us take a sample *abcd* chat image through surfing [5],

Figure 2: Youth Attractive Video Chat

Table 1
Computation Table for *abcd* Video Chat Webportal

a, =1–9/10= -0.8 –ve Value	b, =2–8/10=–0.6 –ve Value
c, =8/10=0.8 (80 % Uncertainty)	d, = a + b /10=0.14
e, = b + c /10=0.14	x, = c+ a/10=0.16
y=(a + b+ c+ d+ e +x)/10 =0.264	$r(X)$=(0.1+0.3+0.4+0.5+0.6+ 0.7 +0.8 +0.9) /10 =0.43
$f(X)$=(0.9 +0.8+0.7+0.6+ 0.5+0.4+0.3)/10 = 0.42	$u(X)$=(0.1+0.2+0.3+0.4+ 0.5+0.7+0.8+0.9) /10=0.39
R– 0.344,	F– 0.252,
U– 0.312,	RF–Max(.344,.252)+0.14=0.48
FU–Max(.42,.39)+0.14=0.56,	RU–Max(.344,.312)+0.16=0.504
RFU-Max(.344,.252,.312,.48,.56,.504)+0.264=0.824 (RAW)	
D_f=1/2*((0.824+0.8))=0.812 (MOULDED)	

Therefore 81.2% deceptive video chat. More than 50% represents the deceptive rating so we kindly avoid chatting and confirm it with the corresponding authority.

Then we verify the second chat server from Yahoo messenger [6] as follows,

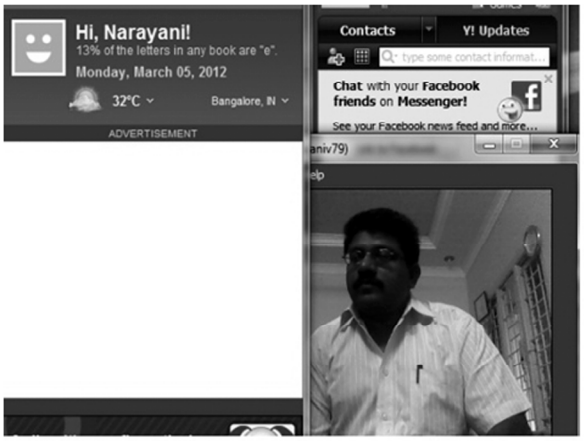

Figure 3: Privacy Chat using Yahoo Messenger

Table 2
Computation Table for Yahoo Messenger

a =10–1/10= 0.9	b =10–1/10= 0.9
c =1/10=0.1 (10 % Uncertainty)	d =0.18
e =0.1	x =0.1
y=0.68/10=.068	$r(X)$=(0.1) /10=0.01
$f(X)$=(0.9)/10= 0.09	$u(X)$=0.1/10=0.01
R=.001,	F=0.009,
U=0.001,	RF–0.189,
FU–0.109,	RU–0.101,
***RFU*–0.027+0.068=0.095**	
D_f=1/2*((0.095+0.18))=0.275	

5. RESULTS AND DISCUSSION

While comparing the analysis results for the two video surfing entity portals, we are in the situation of avoiding dangerous portal address for a genuine and safer chatting system. Confirming the web portal address and following the verifications definitely keep us in safer surfing. The results are as follows:

Table 3
Results Table for *abcd* Vidoechatportal

Component Implementation	*Deception Detection Level*
Randomization	34.4 %
Fuzzification	25.2 %
Uncertainty	31.2 %
Randomization & Fuzzification	48 %
Fuzzification & Uncertainty	56 %
Randomization & Uncertainty	50.4 %
Randomization, Fuzzification & Uncertainty	81.2 %

Table 4
Results Table for Yahoo Messenger Webportal

Component Implementation	*Deception Detection Level*
Randomization	0.1 %
Fuzzification	0.9 %
Uncertainty	0.1 %
Randomization & Fuzzification	18.9 %
Fuzzification & Uncertainty	10.9 %
Randomization & Uncertainty	10.1 %
Randomization, Fuzzification & Uncertainty	27.5 %

The proposed model identifies the deceptive Video chat portal and genuine video chat portal with a variant level as 81% and 28 % deficiency approximately. When the final result of RFU-Randomized, Fuzzy Uncertainty Evaluation crosses 50%, it is the responsibility of the browser or user to skip the process immediately. Our proposed model produces only the maximum efficiency rate as 99 % with the concrete result as proceed or not to proceed further.

6. CONCLUSION

Nowadays the teenage people are very well versed with the recent features of electronic communication media syndromes. Sophisticated devices and vast online portals attracted them with ethical or non ethical strategies [3]. Detecting deception for the video yakking portals are now being a tedious process due to the implementation of advanced techniques. But when we implement the tools of predictability from the unpredictable strategies such as Mathematical randomization, Fuzzy logic, Uncertainty, Genetic algorithm etc, it is possible to detect the deception level with some level of efficiency.

In the experiment domain we used abcd sexy video chat for identifying the deceptions. The proposed model can be evaluated in any video chat domains for the accuracy of deception detection in its core schema.

The individual application of predictable tools provide less efficiency than with the combined application In this research we identified that the individual application provides 35 % efficiency then the Combination of two applications provides 65 % efficiency finally the fusional application of three strategies provides 95% efficiency.

In near future we will try to implement Deception detection techniques with the combined approach of Mathematical Randomization, Fuzzy logic, Uncertainty, Genetic algorithm and artificial intelligence to attain 100 % efficiency.

REFERENCES

[1] Bond,C.F. "A World of Lies: The Global Deception Research Team", *Journal of Cross-culture Psychology*, 2006, **37(1)**, 60-74.

[2] Bruce Luber, Carl Fisher, Paul S. Appelbaum, Marcus Ploesser and Sarah H. Lisanby, "Non-Invasive Brain Stimulation in the Detection of Deception: Scientific Challenges and Ethical Consequences", *Behavioral Sciences and the Law Behav*. Sci. Law 27: 191-208 (2009) Published online 5 March 2009 in Wiley Inter Science-(www.interscience.wiley.com) DOI: 10.1002/bsl.860

[3] Burgeon J.K., and Qin T. "The Dynamic Nature of Deceptive Verbal Communication". *Journal of Language and Social Psychology*, 2006, **25(1)**, 1-22.

[4] Steve Woznaik, Kevin D. Mitnick, William L. Simon, 2002. "The Art of Deception: Controlling the Human Element of Security". Wiley; 1 Edition.

[5] http://sexy-video-chat.com/

[6] in.messenger.yahoo.com/