

بنام خدا

دانشگاه بین المللی امام رضا (ع)

گروه کامپیوتر

تابع چگالی سیکنال پنهان سازی شده در

روش مدولاسیون اندیس کوادرنریاسیون اسکالر

درس:

اختفاء اطلاعات

تهیه کننده:

دکتر رضا صمدی

دی ماه ۹۴

در این گزارش قصد دارم پیاده سازی تابع چگالی سیگنال پنهان سازی شده در روش مدولاسیون اندیس کوانتیزاسیون اسکالر را بیان کنم. ابتدا فرمول ها را مرور کرده و سپس پیاده سازی در نرم افزار متلب را با رسم شکل نشان خواهم داد.

سیگنال پنهان سازی شده در روش مدولاسیون اندیس کوانتیزاسیون اسکالر به صورت زیر است:

$$\begin{aligned}
 y &= x - \alpha e_{m,k}(x) \\
 e_{m,k}(x) &= x - Q_{\Delta_m}(x) \\
 Q_{\Delta_m}(x) &= Q_{\Delta}(x - \Delta \frac{m}{p} - k) + \Delta \frac{m}{p} + k \\
 \Delta &> 0 \\
 0 &\leq \alpha \leq 1 \\
 m &\in \{0, \dots, p-1\}
 \end{aligned}$$

هدف محاسبه تابع چگالی سیگنال پنهان سازی شده به شرط معلوم بودن پیام، با فرض داشتن تابع چگالی میزبان است. اگر مراکز کوانتیزاسیون شیفت یافته به صورت زیر تعریف شوند:

$$\begin{aligned}
 c_{n,m} &\triangleq n\Delta + \Delta \frac{m}{p} + k \quad \text{where } n \in \mathbb{Z} \\
 x_{n,m}^{\pm} &\triangleq c_{n,m} \pm \frac{\Delta}{2} \\
 y_{n,m}^{\pm} &\triangleq c_{n,m} \pm (1-\alpha) \frac{\Delta}{2}
 \end{aligned}$$

آنگاه اثبات می شود که تابع چگالی سیگنال پنهان سازی شده به شرط معلوم بودن پیام به شکل زیر خواهد شد.

$$f_{Y|M}(y | M = m) = \sum_{n=-\infty}^{+\infty} \frac{f_X(c_{n,m} + \frac{y - c_{n,m}}{1-\alpha} | y_{n,m}^- < y \leq y_{n,m}^+)}{1-\alpha} (F_X(x_{n,m}^+) - F_X(x_{n,m}^-))$$

با توجه به این رابطه

$$\Pr(y_{n,m}^- < y \leq y_{n,m}^+) = \Pr(x_{n,m}^- < y \leq x_{n,m}^+) = F_X(x_{n,m}^+) - F_X(x_{n,m}^-)$$

می توان تابع چگالی سیگنال پنهان سازی شده به شرط معلوم بودن پیام را به شکل زیر هم نوشت.

$$f_{Y|M}(y | M = m) = \sum_{n=-\infty}^{+\infty} \frac{f_X(c_{n,m} + \frac{y - c_{n,m}}{1 - \alpha}, y_{n,m}^- < y \leq y_{n,m}^+)}{1 - \alpha}$$

در نهایت تابع چگالی سیگنال پنهان سازی شده به صورت زیر حاصل می شود.

$$f_Y(y) = \sum_{m=0}^{p-1} \Pr(M = m) f_{Y|M}(y | M = m)$$

پیاده سازی نرم افزاری مباحث بالا در نرم افزار متلب در زیر آمده است. در این پیاده سازی، تابع pdf\_y وظیفه تولید تابع چگالی سیگنال پنهان سازی شده به شرط معلوم بودن پیام را دارد.

```
function main
set(0, 'DefaultAxesFontSize', 14, ...
    'defaultlinelength', 3, ...
    'DefaultAxesLineWidth', 0.5)
d = 1;           %delta
a = 0.75;       %alpha
p = 2;          %number of messages
k = -d / 4;     %key
s = 1;          %std of x
y_m = 4 * s + d; %maximum of y
y = linspace(-y_m, y_m, 1e4);
py_0 = pdf_y(y, d, 0, p, k, a, s);
py_1 = pdf_y(y, d, 1, p, k, a, s);
p_y = 0.5 * py_0 + 0.5 * py_1;
p_x = normpdf(y, 0, s);

figure, plot(y, py_0, y, py_1)
legend('p_Y(y|M=0)', 'p_Y(y|M=1)')
title(['\Delta = ' num2str(d) ...
    ', \alpha = ' num2str(a) ...
    ', \sigma_X = ' num2str(s)])
figure, plot(y, p_x, y, p_y)
legend('p_Y(y)', 'p_X(x)')
title(['\Delta = ' num2str(d) ...
    ', \alpha = ' num2str(a) ...
    ', \sigma_X = ' num2str(s)])
end

function py = pdf_y(y, d, m, p, k, a, s)
% d ~ delta
% m ~ message
% p ~ number of messages
% k ~ key
% a ~ alpha
% s ~ std of x
```

```
py = zeros(size(y));  
n_max = ceil(max(abs(y)) / d);  
for n = -n_max : n_max;  
    cnm = n * d + d * m / p + k;  
    I = abs(y - cnm) <= ((1 - a) * d / 2);  
    py(I) = normpdf(cnm + (y(I) - cnm) / (1 - a), 0, s) / (1 -  
a);  
end  
end
```

در حالت باینری  $p = 2$  توابع چگالی سیگنال پنهان سازی شده به شرط معلوم بودن پیام برای مقادیر مختلف آلفا در شکل های زیر رسم شده است. همچنین به مقایسه توابع چگالی سیگنال پنهان سازی شده و سیگنال میزبان برای مقادیر مختلف آلفا توجه کنید.





