

فصل ۱

نهان کاوی با استفاده از تحلیل مقادیر تکین و تخمین نویز

۱.۱ مقدمه

۱.۱.۱ تجزیه مقادیر تکین

تجزیه مقادیر تکین^۱، یکی از مهم ترین تجزیه ها برای ماتریس های حقیقی و مختلط به شمار می آید. SVD کاربرد فراوانی در زمینه محاسبه ماتریس های شبه معکوس، تخمین کوچکترین مربع، تخمین ماتریس و ... دارد. برای ورود به این مبحث فرض کنید که ماتریس M ، ماتریسی است با ابعاد $m \times n$ که عضوی از میدان K است. می توان اثبات کرد که ماتریس M را می توان به صورت زیر تجزیه کرد.

$$M = U \Sigma V^* \quad (1.1)$$

U در رابطه ۱.۱ ماتریسی است $m \times m$ که عضوی از میدان K و Σ ماتریس قطری است که عناصر آن اعداد حقیقی نامنفی هستند. V^* نیز ماتریسی است $n \times n$ و عضو میدان K . به چنین تجزیه ای اصطلاحاً تجزیه مقادیر تکین می گوئیم. در ادامه خواهیم دید که مقادیر تکین در برگیرنده اطلاعات بسیار خوبی از سیگنال^۲ می باشد.

۲.۱.۱ تاثیر نهان نگاری LSB بر روی SVD

ورودی سامانه نهان کاوی را تصویر خاکستری با ابعاد $W \times H$ در نظر بگیرید. در حقیقت سیگنال پوش، به صورت ماتریسی است با ابعاد $W \times H$ که هر عنصر (پیکسل) آن عددی است بین ۰ تا ۲۵۵. در نهان نگاری امن یک کلید

^۱Singular value decomposition

^۲در این جا سیگنال تصویر است

مخفی K در سمت فرستنده و گیرنده موجود می باشد. این کلید را می توان خروجی یک PRNG^3 در نظر گرفت. همان طور که می دانید در پنهان نگاری LSB ، ابتدا مکان هایی را به صورت تصادفی در تصویر انتخاب می کنیم. در مرحله ی بعدی، یک بیت پیام را در سطح بیت هشتم مکان های انتخابی، قرار می دهیم. فرض کنید که پیام M با طول L ، را می خواهیم در تصویر پوش (C) با روش LSB پنهان کنیم. تصویر پنهان نگاری شده حاصل را با S نمایش می دهیم. در این صورت می توان نوشت:

³pseudo-random number generator