# یک رویکرد جدید برای LSB تصویر بر اساس نهان نگاری با استفاده از رمز های کلیدی

**عرفانه نوروزی** [۱,*]

**۱- دانشکده مهندسی کامپیوتر، واحد سپیدان، دانشگاه آزاد اسلامی، سپیدان، ایران**

## چکیده

در این مقاله یک رویکرد معرفی برای بهترین وکم ارزشترین رقم (LSB) بر اساس پنهان کردن درون تصویر ارائه شده که باعث افزایش LSB به منظور بهبود سطح امنیت پنهان نگاری می باشد. این یک رویکرد جدید به جای LSB از تصویر RGB رنگ واقعی می باشد. مفهوم جدید امنیتی پنهان کردن اطلاعات در LSB تصویر با یک کلید مخفی کدگذاری برای محافظت از کاربران غیر مجاز می باشد. به طور کلی در LSB ، پنهان نگاری به یک موقعیت خاص LSB درون تصویر ذخیره می شود. به همین دلیل با دانستن روش بازیابی، هر کسی می تواند پنهان را استخراج نماید. ما از این مقاله، پنهان رابه موقعیت های مختلف از LSB تصویر بسته به کلید های مخفی ذخیره می کنیم. در نتیجه ما از نسبت سیگنال به نویز (PSNR) برای اندازه گیری کیفیت تصاویر stego استفاده می کنیم. ارزش PSNR نتیجه بالاتری می دهد درروش پیشنهادی ما تعداد بسیار کمی از بیت تصویر تغییر می کند. نتایج به دست آمده نشان می دهد که نتایج روش ارائه شده در LSB بر اساس پنهان نگاری تصویر با استفاده از کلید های مخفی فراهم می کند که مسئله امنیت و ارزش PSNR از LSB را بالاتر می برد.

**کلمات کلیدی:** پوشش تصویر، پنهان نگاری، stego تصویر، LSB.

## ۱. مقدمه

در گذشته، مردم از خالکوبی پنهان و یا جوهر نامرئی برای کشف محتوای پنهان نگاری استفاده می کردند. فن آوری امروز، کامپیوتر و شبکه کانال های ارتباطی برای پنهان نگاری اطلاعات می باشد. اما حریم خصوصی یک نگرانی برای بسیاری از افراد در اینترنت است. تصویر نهان نگاری برای دو طرف برقراری ارتباط مخفیانه و محرمانه را مهیا می کند. پنهان نگاری یک تکنیک برای مخفی کردن اطلاعات از ناظر به ایجاد یک ارتباط نامرئی است[۱]. به طور کلی، استقرار یک سیستم متشکل از رسانه های پوشش را که در آن اطلاعات محرمانه تعبیه شده است. روند تعبیه تولید یک رسانه stego با جایگزین

**دانشکده مهندسی کامپیوتر، واحد سپیدان، دانشگاه آزاد اسلامی، سپیدان، ایران**
**Email: noroozierfaneh@gmail.com***

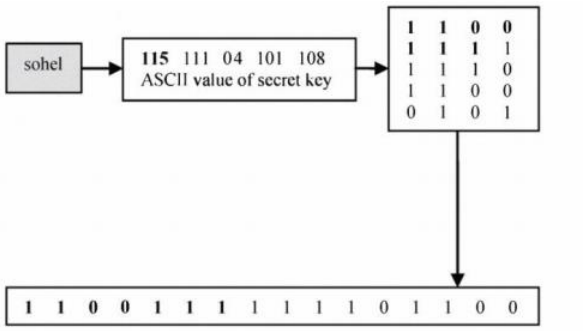
کردن اطلاعات با استفاده از داده پیام های پنهان است. برای مخفی کردن اطلاعات پنهان، پنهان نگاری یک فرصت بزرگ در چنین راهی که کسی می تواند حضور این پیام مخفی دهد[۲].

به طور کلی اطلاعات محرمانه به موقعیت خاص از کم ارزشترین رقم (LSB)درون یک تصویر پوشش است که حامل پیام های ذخیره شده می باشد [۱، ۲، ۳، ۴]. هر کسی می تواند اطمینان کند که موقعیت خاص از LSB حاوی اطلاعات محرمانه می باشد. پس از آن برای بازیابی اطلاعات محرمانه برای هر کسی با استفاده از روش بازیابی آسان است ،هدف اصلی پنهان نگاری تصویر اطمینان از امنیت اطلاعات پنهان است. برای هدف امنیتی، ما یک رویکرد جدید از LSB بر اساس پنهان نگاری تصویر ارائه می دهیم. در اینجا ما در حال اضافه کردن یک کلید خصوصی که اطمینان از امنیت اطلاعات پنهان شده است. درج اطلاعات پنهان کاملا توسط کلید های مخفی کنترل می شود. این کلید مخفی تصمیم می گیرد موقعیت مناسب از اطلاعات پنهان شده می باشد که بازیابی اطلاعات مخفی بدون کلید مخفی دشوار است. بنابراین با استفاده از یک کلید مخفی، ما می توانیم سطح امنیت اطلاعات پنهان در LSB بر اساس پنهان نگاری تصویر را افزایش دهیم. تعدادی از تحقیقات موجود توصیف ویژگی های پنهان نگاری تصویر وجود دارد. بسیاری از روشهای پنهان نگاری پیشنهاد شده است [۲، ۳، ۴، ۵، ۶]. شایع ترین این جایگزین کردن حداقل بیت یا (LSB)از پیکسل با پیام های مخفی LSB. شناخته شده بر اساس پنهان نگاری [۳] تصویر در ارائه شده که یک روش تطبیقی بر اساس رابطه بین پیکسل ها می باشد. این روش تا حد زیادی افزایش کیفیت stego تصویراست که ممکن است به بازیابی اطلاعات محرمانه برای هر کسی با استفاده از روش بازیابی صورت پذیرد. یکی دیگر از LSB بر اساس پنهان نگاری تصویر در [۲] و پیشنهاد سه روش پنهان نگاری کارآمد است که استفاده از این اطلاعات برآورد مقدار را به یک پیکسل ورودی تصویر پوشش داده و قراردادن ثابت سه بیت از اطلاعات در مناطق صاف تعبیه شده ارائه شده و تعداد متغیری از بیت ها را به مناطق پوششی تعبیه شده است. این روش با استفاده از برخی پیکسل های تصویر برای ذخیره بیش از حد بیت ها از اطلاعات پنهان دیگر پیکسل بدون تغییر باقی می ماند. به عنوان یک نتیجه، برخی از پیکسل ها تقریبا تحریف اما دیگر پیکسل استفاده نشده است. آنها همچنین هیچ مشکل امنیتی فراهم نمی آورند و ممکن است برای بازیابی اطلاعات محرمانه برای هر کسی مورد استفاده واقع شود. در این مقاله، یک روش کارآمد LSB بر اساس پنهان نگاری که با بهره گیری از کلید های مخفی برای پنهان کردن اطلاعات به یک پیکسل ورودی تصویر پوشش بدون تحریف متن اصلی ارائه شده است. در اینجا یک بیت از اطلاعات پنهان در هر دو LSB ماتریس سبز یا آبی با یک پیکسل خاص است که توسط کلید مخفی قرار داده شده بنابراین هر کسی می تواند دقیقا کمی از اطلاعات مخفی در هر دو LSB سبز یا ماتریس آبی قرار دهد.در نتیجه، سطح امنیت پنهان نگاری تصویر به دست می آید.

## ۲. بررسی ادبیات

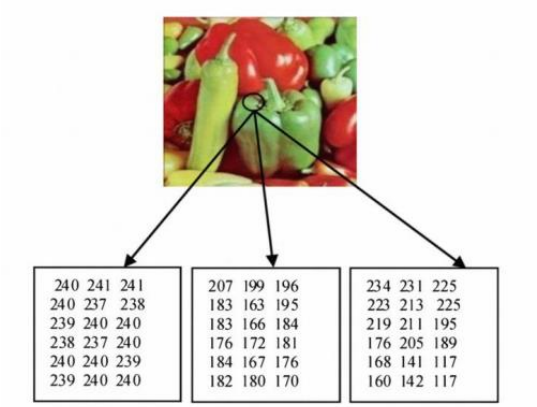
ساده ترین روش برای مخفی کردن داده ها در یک تصویر کم ارزش بیت (LSB) درج نامیده می شود. برای تصویر ۲۴ بیت رنگ واقعی، مقدار حداقل و تغییرات نامحسوس به چشم انسان خواهد آمد.

برای اندازه گیری کیفیت stego تصویر، نویز سیگنال در برابر (PSNR) محاسبه شده است. اندازه گیری آماری PSNR مورد استفاده برای تصویر دیجیتال یا ارزیابی کیفیت فیلم است. [۲]




**شکل ۱ – تبدیل اطلاعات پنهان برآرایه**

یک طرح رنگ ۲۴ بیتی با استفاده از ۲۴ بیت در هر پیکسل و هر بایت نشان دهنده شدت سه رنگ اصلی قرمز، سبز، و آبی (RGB) بود. بنابراین، یک تصویر پوشش را می توان به سه ماتریس تقسیم همانطور که در شکل نشان داده شده است تقسیم نمود.اطلاعات پنهان از دهدهی به دودویی تبدیل شده است. هر پیکسل به مقدار باینری ۸ بیتی تبدیل شده است و سپس ۲۰ آرایه به آرایه ID تغییر داده است که از اطلاعات مخفی نامیده می شود. این فرایند برای تبدیل اطلاعات پنهان برآرایهD۱ در شکل زیر نشان داده شده است.اطلاعات پنهان از دهدهی به دودویی تبدیل شده است. هر پیکسل به مقدار باینری ۸ بیتی تبدیل شده است و سپس ۲۰ آرایه به آرایه ID تغییر داده است که از اطلاعات مخفی نامیده می شود. این فرایند برای تبدیل اطلاعات پنهان برآرایهD۱ در شکل زیر نشان داده شده است.



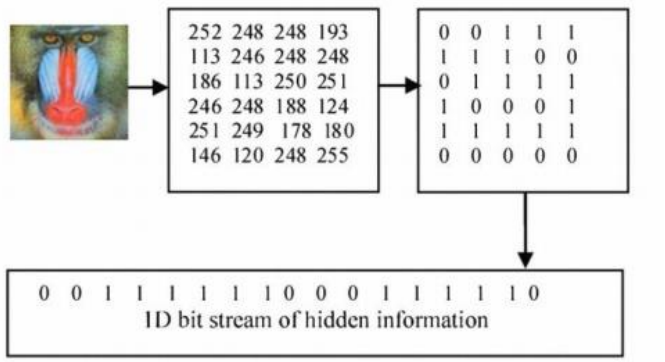

**شکل ۲ – RGB نمایش ماتریسی از یک تصویر پوشش**

در واقع شرایط کاهش اعوجاج از ارزش PSNR بزرگتراحتمال حمله های بصری با چشم انسان راکاهش می دهد[۲][۳].

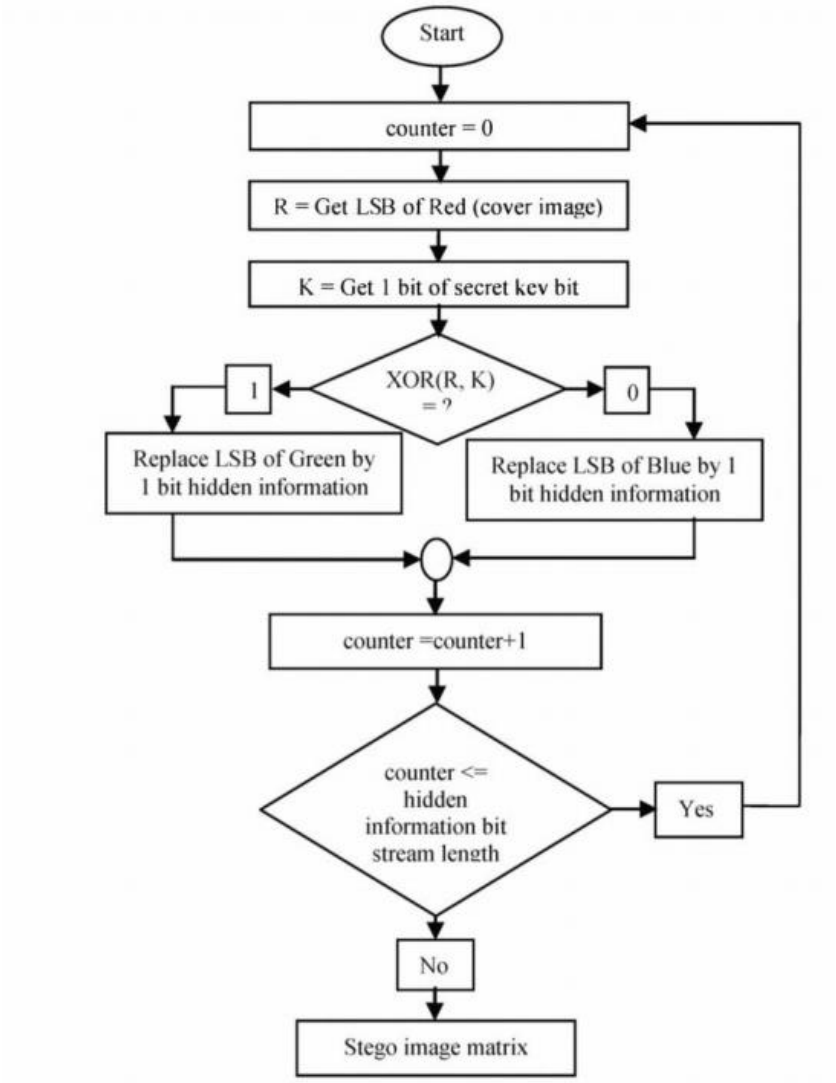
۲۴۰ ۲۴۰ ۲۳۹
۱۷۰ ۱۸۰ ۱۸۲
۱۱۷ ۱۴۲ ۱۶۰

## ۳. روشهای پیشنهادی

در این مقاله، نمایش دودویی از اطلاعات پنهان گرفته و بازنویسی LSB هر بایت در تصویر پوشش استفاده می شود. در اینجا ما یک کلید مخفی معرفی می نماییم. تکنیک پنهان کردن اطلاعات پنهان،برای مخفی کردن اطلاعات به یک تصویر پوشش ادغام می کنیم. این تصویر پوشش به سه ماتریس (قرمز، سبز و آبی) همانطور که در شکل نشان داده شده است تقسیم شده است. کلید های مخفی به تبدیل آرایه IO از جریان کمی یا کلید های مخفی و ماتریس قرمز برای تصمیم گیری به جای اطلاعات پنهان ماتریس سبزو هم ماتریس آبی استفاده می شود. هر بیت از کلید های مخفی XOR با هر LSB ماتریس قرمز یکسان است. همین روند ادامه می یابد تا زمانی که این اطلاعات پنهان به پایان رسید. نمودار جریان برای مخفی کردن اطلاعات پنهان درون تصویر پوشش در شکل ۳ نشان داده شده است.

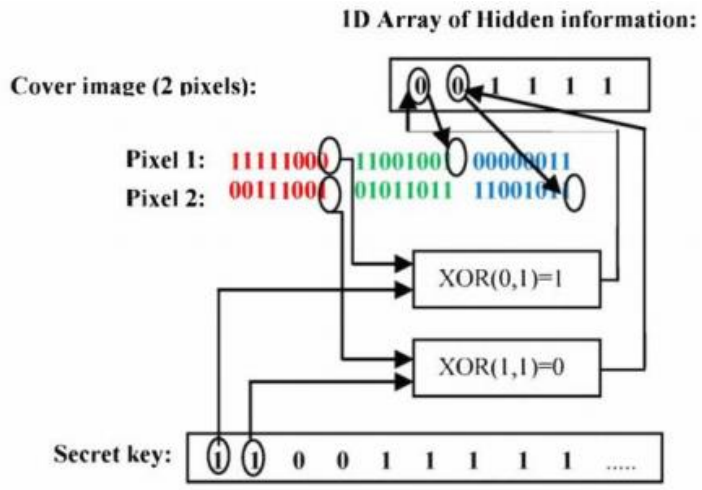



**شکل ۳ – نمودار جریان برای مخفی کردن اطلاعات پنهان درون تصویر پوشش**




**شکل ۴ – LSB ماتریس سبز جایگزین توسط اولین بیت**

در شکل ۴، LSB ماتریس رنگ قرمز پیکسل است و اولین بیت از کلید های مخفی ارزش XOR از O است در روش ما، اگر ارزش XOR و سپس LSB ماتریس سبز جایگزین توسط اولین بیت از اطلاعات پنهان می گردد. اگر مقدار XOR برابر با صفر و سپس LSB ماتریس رنگ قرمز اولین بیت از اطلاعات مخفی جایگزین شده است. آرایه IO از کلید های مخفی دایره ای است. این فرایند تعویض بسته خواهد شد و از اطلاعات مخفی ۱۰ آرایه ادامه دارد.




**شکل ۵ – نمایندگی آرایه ای از اولین بیت کلید های مخفی**

آرایه ID از اطلاعات پنهان:
پیکسل ۱: 1111100 :
پیکسل ۲: ۰۰۱۱۱۰۰
کلید های مخفی: ۰ ۰

در شکل ۵، LSB ماتریس قرمز پیکسل ۰،۱ O است وارزش XOR از O است و در روش ما، ارزش XOR و سپس LSB ماتریس سبز جایگزین توسط اولین بیت از اطلاعات پنهان است. اگر مقدارXOR برابر صفر و سپس LSB ماتریس قرمز اولین بیت از اطلاعات مخفی جایگزین شده است. آرایه IO از کلید های مخفی دایره ای است. این فرایند بسته به طول آرایه IO اطلاعات پنهان را تعویض خواهد نمود.

### ۳. بازیابی تکنیک از اطلاعات مخفی

بازیابی اطلاعات پنهان از یک تصویر stego می باشد. این تصویر stego به سه ماتریس (قرمز، سبز و آبی) همانطور که در شکل ۲ نشان داده شده است تقسیم شده است. سپس ما باید بدانیم که کلید های مخفی به IO جریان کمی آرایه تبدیل شده است. هر بیت از کلید های مخفی XOR با هر LSB قرمز ماتریس تصویر stego است.

در نتیجه ارزش XOR تصمیم می گیرد که از اطلاعات مخفی بیتی در هر دو LSB ماتریس سبز یا ماتریس آبی از تصویر stego ذخیره شده است. طول این اطلاعات در سطر اول از stego تصویر در طول فرایند ذخیره می شود. روند بهبودی بسته به طول پنهان جریان کمی اطلاعات ادامه نمودار جریان برای بازیابی اطلاعات پنهان از stego تصویر نشان داده شده است.

در شکل ۵، LSB ماتریس قرمز پیکسل ۰است و اولین بیت از کلید های مخفی ارزش XOR است پس از آن به صورت پنهان می توان دریافت LSB ماتریس سبز. اگر مقدار XOR O است و سپس داده پنهان را می توان در LSB ماتریس آبی

یافت. این بیت را برداشت و ذخیره کرد به یک آرایه ID. در نهایت آرایه IO به ۲۰ آرایه تغییر شکل اطلاعات واقعی است [7]. این فرایند برای بازیابی اطلاعات پنهان از stego تصویر است. آرایه IO از جریان کمی کلید های مخفی و ماتریس رنگ قرمز تنها برای تصمیم گیری به جای اطلاعات پنهان که هم از ماتریس سبز یا ماتریس آبی استفاده می شود.هر بیت از کلید های مخفی XOR با هر LSB ماتریس قرمز است. همین روند ادامه می یابد تا زمانی که این اطلاعات پنهان را به پایان رساند. نمودار جریان برای مخفی کردن اطلاعات پنهان به تصویر پوشش در شکل ۵ نشان داده شده است. با استفاده از معادله و ارزش (PSNR)، محاسبه stego تصویر. این مقادیر PSNR در جدول 1 نمایش داده شده است.

**جدول ۱- نتایج تجربی برای روش ارائه شده**

| Cover Images | PSNR (in dB) in Na-I Wu's method | PSNR (in dB) in Four Neighbor method | PSNR (in dB) in our method |
|---|---|---|---|
| Lena | 34.3962 | 41.1468 | 53.7618 |
| Baboon | 30.413 | 36.5154 | 53.7558 |
| Peppers | 33.7496 | 41.0315 | 53.7869 |

تصاویر
PSNR (در دسی بل)
لنا
۵۳,۷۶۱۸
شکل بابون
۵۳,۷۵۵۸
فلفل
۵۳,۷۸۶۹

نتایج تجربی با استفاده از روش پیشنهادی ما بر روی تصاویر مختلف استاندارد با روش های دیگر بررسی کرده اند. روش NA-I و[۳] تغییر پیکسل بیشتر (تقریبا همه از پیکسل های یک تصویر) از یک تصویر در پنهان کردن اطلاعات. چهار همسایه، هشت همسایه و روش همسایه مورب [۲] ۳ تغییر یا چند بیت از یک پیکسل. اما برای همان ظرفیت طرح پیشنهادی ما تغییر تنها یک بیت از هر پیکسل است.

جدول ۱مقایسه نتایج با استفاده از روش NA-I و چهار روش همسایه
تصاویر پوشش
PSNR (در دسی بل) در روش PSNR (در دسی بل) در روش Neighbor چهار

PSNR (در دسی بل)

در روش لنا
۳۴,۳۹۶۲
۴۱,۱۴۶۸
۵۳,۷۶۱۸
شکل بابون
۳۰,۴۱۳
۳۶,۵۱۵۴
۵۳,۷۵۵۸
فلفل
۳۳,۷۴۹۶
۴۱,۰۳۱۵
۵۳,۷۸۶۹

نکته دیگر این است که بدون کلید مخفی هیچ کس قادر به دانستن موقعیت دقیق که در آن اطلاعات پنهان قرار داده شده است. از آنجا که هر بیت از اطلاعات پنهان یا در LSB ماتریس سبز یا ماتریس آبی قرار داده است. بنابراین، به استخراج اطلاعات پنهان، کلید مخفی مورد نیاز است. همانطور که ما تنها یک بیت از LSB از سبز یا آبی را در هر پیکسل از تصویر پوشش تغییر می کند، بنابراین نتیجه ارزش PSNR روش پیشنهادی بهتر از روش های دیگر است. بنابراین روش ارائه یک راه موثر برای قرار دادن اطلاعات پنهان به تصویر پوشش بدون اعوجاج می نماید.

## ۱۲. نتیجه‌گیری

نتایج تجربی نشان می دهد که روش ارائه یک راه موثر برای یکپارچه سازی اطلاعات پنهان گزارش بدون اعوجاج قابل توجه است. برای کاربران غیر مجاز جهت شناسایی تغییرات در تصویرstego بسیار دشوار است. استفاده از کلید های مخفی یک راه برای حفظ اطلاعات از کاربر غیر قانونی می باشد. در روش پیشنهادی با استفاده از کلید های مخفی جهت پنهان کردن اطلاعات پنهان به تصویر را پوشش میدهد. این فرایند یک بعد جدید برای پنهان نگاری تصویر فراهم می کند. بازیابی اطلاعات پنهان برای شخص ثالث بدون دانستن کلید مخفی دشوار است روش پیشنهادی ما ارزش بهتر PSNR بزرگتر را نشان می دهد با کیفیت بهتر از تصویر و یا در شرایط دیگر اعوجاج پایین تر است.

## مراجع

[1] Islam, R., Naji, A. W., Zaidan, A. A., & Zaidan, B. B. (2010). New System for Secure Cover File of Hidden Data in the Image Page within Executable File Using Statistical Steganography Techniques. arXiv preprint arXiv:1002.2416.

[2] Koscielny, C., Kurkowski, M., & Srebrny, M. (2013). An Electronic Signature and Hash Functions. In Modern Cryptography Primer (pp. 127-145). Springer Berlin Heidelberg.

[3] Mahdi, O. A., Mohammed, M. A., Mohamed, A. J., & Baghdad, I. (2012). Implementing a Novel Approach an Convert Audio Compression to Text Coding via Hybrid Technique.

[4] Makbol, N. M., & Khoo, B. E. (2013). Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. AEU-International Journal of Electronics and Communications, 67(2), 102-112.

[5] Nandi, M. and S. Paul (2010). Speeding up the wide-pipe: Secure and fast hashing. Progress in Cryptology-INDOCRYPT 2010, Springer: 144-162.

[6] Park, J. M., Chong, E. K., & Siegel, H. J. (2002). Efficient multicast packet authentication using signature amortization. In Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on (pp. 227-240). IEEE.

[7] Prabakaran, G., Bhavani, R., & Kanimozhi, K. (2013, February). Dual transform based steganography using wavelet families and statistical methods. In Pattern Recognition, Informatics and Medical Engineering (PRIME), 2013 International Conference on (pp. 287-293). IEEE.