انجمن رمز ایران
Iranian Society of Cryptology
چهارمین کنفرانس انجمن رمز ایران
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران

ارائه مدل ریاضی روش‌های پنهان‌نگاری LSB-M و LSB-F

مجتبی مهدوی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان
mahdavi@ec.iut.ac.ir

شادرخ سماوی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان
samavi96@cc.iut.ac.ir

وجیهه ثابتی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان
sabeti@ec.iut.ac.ir

چکیده: الگوریتم‌های جاسازی در بیت کم ارزش پیکسل‌های تصویر (*LSB-F* و *LSB-M*) از رایج‌ترین و ساده‌ترین روش‌های پنهان-نگاری است. در این مقاله مدلی ریاضی برای این روش‌ها ارائه شده است. این مدل می‌تواند برای توجیه رفتار و خواص این دو نوع پنهان‌نگاری بکار رود. هیستوگرام تصویر یکی از ویژگی‌های تصویر است که در اثر استفاده از روش‌های پنهان‌نگاری تغییر می‌کند. با استفاده از مدل ریاضی ارائه شده، رفتار هیستوگرام تصویر بعد از جاسازی نیز مدل شده است. سپس از مدل هیستوگرام تصویر، برای تخمین میزان تغییرات هیستوگرام در اثر جاسازی استفاده گردیده است. صحت مدل‌های ارائه شده توسط شبیه‌سازی به اثبات رسیده است.

واژه های کلیدی: پنهان نگاری، هیستوگرام، مدل ریاضی، بیت کم ارزش

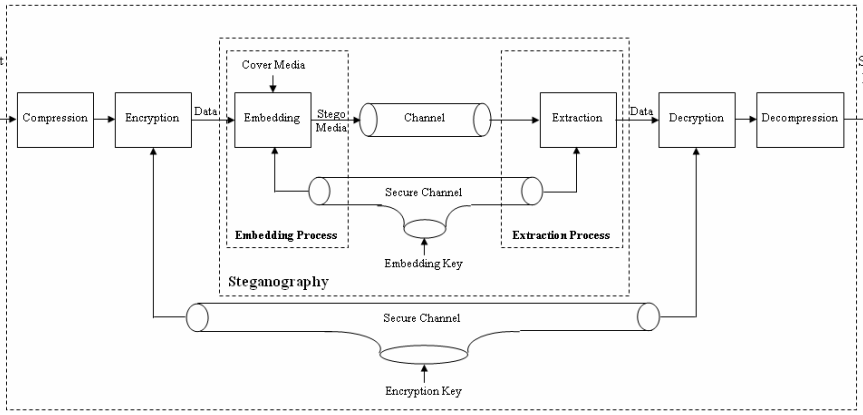
۱- مقدمه

متن، تصویر، صوت و ویدئو را می‌توان به صورت داده‌های دیجیتال بیان کرد. فراگیری فزاینده و رشد سریع استفاده از اینترنت انسان‌ها را به سوی جهان دیجیتال و ارتباط از طریق داده‌های دیجیتال سوق داده است. امنیت ارتباطات دانشی است که شامل علوم مختلفی چون رمزنگاری[1]، تهنقش-نگاری[2]، ارتباطات پوشیده[3] و ... می‌باشد[1].

پنهان نگاری هنر ارتباط پنهانی است و هدف آن پنهان کردن ارتباط به وسیله قرار دادن پیام در یک رسانه پوشانه[4] است به گونه ای که کمترین تغییر قابل کشف را در آن ایجاد نماید و نتوان موجودیت پیام پنهان در رسانه را حتی به صورت احتمالی آشکار ساخت [2].

رمزنگاری نیز یکی از روش‌های امن کردن ارتباطات است. در رمزنگاری تلاشی برای پنهان کردن پیام کد شده انجام نمی‌شود و هدف، انتقال اطلاعات به گونه‌ای است که طرف

1 Cryptography
2 Watermarking
3 Covert Channel
4 Cover media



شکل ۱: شمای کلی یک ارتباط سری با استفاده از پنهان‌نگاری

سوم قادر به خواندن آن نباشد. اما، پنهان نگاری پیام رمز را تغییر نمی‌دهد، بلکه آن را داخل یک شئ پوشانه به گونه‌ای مخفی می‌کند که قابل دیدن نباشد[3].

در شکل ۱، شمای کلی یک ارتباط سری با استفاده از پنهان نگاری نشان داده شده است. هدف در این ارتباط تبادل یک پیام سری است. این پیام علیرغم شکل ظاهری خود باید به صورت یک رشته بیتی بیان شود. استفاده از دو ماژول فشرده-سازی[۵] و رمزنگاری[۶] قبل از اعمال روش پنهان‌نگاری الزامی است. فشرده کردن باعث حذف افزونگی‌های موجود در داده و در نتیجه جلوگیری از اتلاف ظرفیت تصویر می‌شود. برای افزایش امنیت ارتباط، یک الگوریتم رمزنگاری برای پنهان کردن مفهوم پیام، روی داده فشرده شده اعمال می‌شود.

به طور کلی روش‌های پنهان‌نگاری از دو فرآیند جاسازی[۷] و استخراج[۸] تشکیل شده‌اند. در فرآیند جاسازی، داده فشرده شده و رمزشده با استفاده از یک الگوریتم جاسازی در یک رسانه پوشانه پنهان می‌شود و رسانه گنجانه[۹] تولید می‌شود. برای افزایش امنیت معمولاً از یک کلید جاسازی در این مرحله استفاده می‌شود. گیرنده با استفاده از یک الگوریتم استخراج، داده مخفی شده را از رسانه گنجانه خارج می‌کند. گیرنده برای خارج کردن پیام اصلی، باید الگوریتم‌های رمزگشایی[۱۰] و سپس بازگشایی[۱۱] را روی پیام استخراج شده اعمال کند[4].

هدف پنهان‌نگاری، غیرقابل کشف بودن وجود داده پنهان شده است، اما اکثر روش‌های پنهان‌نگاری اثرات قابل کشفی در شئ پوشانه باقی می‌گذارند. استفاده از این تغییرات برای کشف وجود یک پیام مخفی در یک ارتباط، هدف پنهان-شکنی[۱۲] است[5].

کارهای زیادی در زمینه پنهان‌نگاری و پنهان‌شکنی در تصاویر انجام شده است. پنهان‌نگاری معمولاً در دو حوزه مکان[۱۳] و حوزه تبدیل[۱۴] صورت می‌گیرد. برای مثال جاسازی داده‌ها در بیت‌های کم ارزش تصاویر[6,7] از حوزه مکان و روش‌هایی مانند *Jsteg*، *OutGuess* و *F5* [9,8,5] از حوزه تبدیل استفاده می‌کنند.

در این مقاله سعی گردیده است تا یک مدل ریاضی برای رفتار روش‌های پنهان نگاری *LSB-F*[۱۵] و *LSB-M*[۱۶] ارائه گردد. چنین مدلی می‌تواند در توجیه رفتار و خواص و سطح امنیت و ظرفیت این نوع پنهان نگاری بکار رود. هیستوگرام تصویر یکی از ویژگی‌هایی است که در جاسازی تغییر می‌کند و استفاده از تغییرات هیستوگرام مبنای بسیاری از حملات موفق می‌باشد[10]. با استفاده از مدل ریاضی ارائه شده برای

5 Compression
6 Encryption
7 Embedding
8 Extraction
9 Stego Media

10 Decryption
11 Decompression
12 Steganalysis
13 spatial domain
14 transform domain
15 Least Significant Bit Flipping (LSB-F)
16 Least Significant Bit Matching (LSB-M)

هیستوگرام تصویر، تخمینی از تغییر ایجاد شده در هیستوگرام تصویر در اثر جاسازی به روش‌های *LSB-F* و *LSB-M* قابل محاسبه است.

در ادامه مقاله، ابتدا الگوریتم *LSB-M* و *LSB-F* به صورت مختصر بررسی می‌شود. سپس در بخش ۳، مدل ریاضی متناظر با این روش ها ارائه می‌شود. با استفاده از این مدل‌های ریاضی، در بخش ٤ روشی برای محاسبه تخمین خطای هیستوگرام در اثر اعمال این روش‌ها ارائه می‌شود. در بخش۵، نتایج تخمین خطای حاصل از تئوری و شبیه سازی مقایسه می‌شود.

۲- الگوریتم *LSB-F* و *LSB-M*

رایج‌ترین و ساده‌ترین روش جاسازی در حوزه مکانی، روش جاسازی در بیت‌های کم ارزش است که پیام را در کم ارزش-ترین بیت‌های پیکسل‌ها قرار می‌دهد. جاسازی به این روش ساده‌ترین روش پنهان‌نگاری در حوزه مکانی است و روش-های پنهان‌نگاری بسیاری بر مبنای این روال تا به حال ارائه شده است. بصورت کلی، روش‌های پنهان‌نگاری در بیت‌های کم ارزش را در دو دسته *LSB-F* و *LSB-M* می‌توان تقسیم بندی کرد[*11*].

در روش *LSB-F*، تنها کم ارزش‌ترین بیت هر پیکسل تغییر می‌کند. به عبارت دیگر در این روش بیت کم ارزش پیکسل-های تصویر پوشانه با بیت‌های پیام جاگذاری می‌شوند. در روش *LSB-M* نیز هدف یکسان کردن بیت *LSB* پیکسل‌های تصویر با بیت‌های پیام است، اما ممکن است برای رسیدن به این هدف چند بیت پیکسل تغییر یابد. در این روش در صورت تطابق بیت داده با بیت کم ارزش پیکسل، تغییری در پیکسل ایجاد نمی‌شود. در صورت عدم تطابق، مقدار پیکسل به صورت تصادفی کاهش یا افزایش می‌یابد. به همین دلیل این روش با عنوان روش جاسازی ± 1 نیز شناخته می-شود[*12*].

جاسازی به روش *LSB-F*، جفت رنگ ها یا زوج مقادیری[17] در هیستوگرام تصویر ایجاد می‌کند که تعداد رخداد آن‌ها در تصویر برابر است. به همین دلیل این روش در برابر حملاتی آسیب پذیر است که هیستوگرام را بررسی می کنند. برخی از این حملات در [*10,13,14*] آورده شده است. اما با توجه با این‌که روش *LSB-M* از ایجاد *POV* در هیستوگرام جلوگیری می‌کند، در برابر حملات ارائه شده برای *LSB-F* مقاوم است. در مورد *LSB-M* نیز حملات دیگری مطرح گردیده است، اما هیچ کدام از آنها کاملاً موفق نبوده‌اند. برخی از این حملات در [*11,15*] آورده شده است.

۳- مدل ریاضی روش‌های *LSB-F* و *LSB-M*

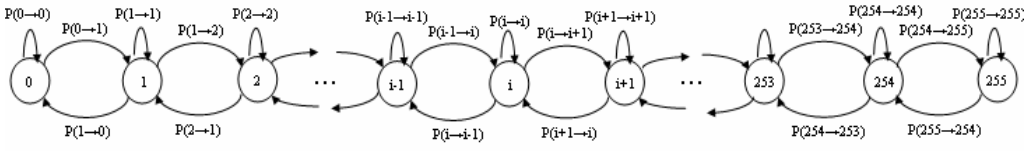
داده‌هایی که در فرآیند جاسازی مورد استفاده قرار می‌گیرند، باید ابتدا فشرده و سپس رمز شوند. داده‌هایی که به این صورت تولید می‌شوند خواصی مانند یک دنباله بیت تصادفی دارند. امید ریاضی تعداد بیت‌های یک و صفر در این رشته بیت با یکدیگر برابر است[*16*]. جاسازی یک بیت داده تصادفی در یک پیکسل باعث ایجاد تغییراتی در مقدار سطح روشنایی آن پیکسل می‌گردد. با توجه به اینکه جاسازی به روش‌های *LSB-M* و *LSB-F* تنها مقدار پیکسل را به اندازه یک واحد کاهش یا افزایش می‌دهد، می‌توان تغییر مقدار سطح روشنایی یک پیکسل در اثر جاسازی یک بیت داده تصادفی را به صورت شکل ۲ مدل کرد.

اگر سطح روشنایی یک پیکسل را i فرض کنیم و سطح روشنایی همین پیکسل بعد از جاسازی در آن را j بنامیم، آنگاه در حالت کلی، با فرض اینکه مقدار داده جاسازی شده d باشد، احتمال تغییر i به j برابر است با:

$$P(i \to j) = P(i \to j \mid d=0)\, P(d=0) + P(i \to j \mid d=1)\, P(d=1)$$

با توجه به الگوریتم بکار رفته برای جاسازی، مقدار این احتمال در حالات مختلف، متفاوت است. در جدول ۱، مقدار این احتمال در حالات گوناگون نشان داده شده است.با توجه به مقادیر بدست آمده در جدول۱، می توان شکل۲ را برای روش *LSB-F* به صورت شکل ۳-الف و برای روش *LSB-M* به صورت شکل ۳-ب نمایش داد.

[17] Pair Of Value (POV)



شکل۲: مدل کلی تغییر مقدار سطح روشنایی یک پیکسل در اثر جاسازی یک بیت داده

در شکل ۳-الف دیده می‌شود که پیکسلی با سطح روشنایی زوج در اثر جاسازی بیت ۱ به سطح روشنایی فرد تغییر می‌کند. در روش *LSB-F*، اگر داده‌های جاسازی شده را تصادفی فرض کنیم پیکسلی با سطح روشنایی $2i$ به احتمال 1/2 به سطح روشنایی $2i+1$ تبدیل می‌شود.

جاسازی به روش *LSB-M* را می‌توان با اضافه شدن اغتشاش[18] به تصویر مدل کرد. تصویر استگو حاصل جمع تصویر پوشانه و نویز گوسی[19] است. در این روش، نویز اضافه شده تنها سه مقدار $+1$، 0 و -1 را می‌تواند داشته باشد. احتمال اضافه شدن هر کدام از این مقادیر بدین صورت است:

$$p(-1)=1/4 \quad , \quad p(0)=1/2 \quad , \quad p(1)=1/4$$

در این صورت با احتمال 1/2 مقدار پیکسل تغییری نمی‌کند ($p(0)=1/2$) و با احتمال 1/4 مقدار پیکسل افزایش ($p(1)=1/4$) یا کاهش ($p(-1)=1/4$) می‌یابد.

حال می‌خواهیم بدانیم اگر الگوریتم *LSB-M* و *LSB-F* را یک بار روی تمام پیکسل‌های تصویر اعمال کنیم، چه تغییراتی در هیستوگرام رنگ پیکسل‌های تصویر بوجود خواهد آمد. در ادامه تصاویر طیف خاکستری[20] مورد بررسی قرار می‌گیرند. روش پیشنهادی را می‌توان برای تصاویر رنگی نیز تعمیم داد، زیرا تصاویر رنگی را می‌توان به صورت سه تصویر طیف خاکستری مجزا در نظر گرفت.

تصویرهای طیف خاکستری با پیکسل‌های ۸ بیتی دارای روشنایی در بازه $[0,255]$ می‌باشند. فرض کنید روشنایی تصویر در موقعیت (m,n) را با $I(m,n)$ نشان دهیم. هیستوگرام، بیانگر فرکانس رخداد هر روشنایی در تصویر است، به عبارت دیگر:

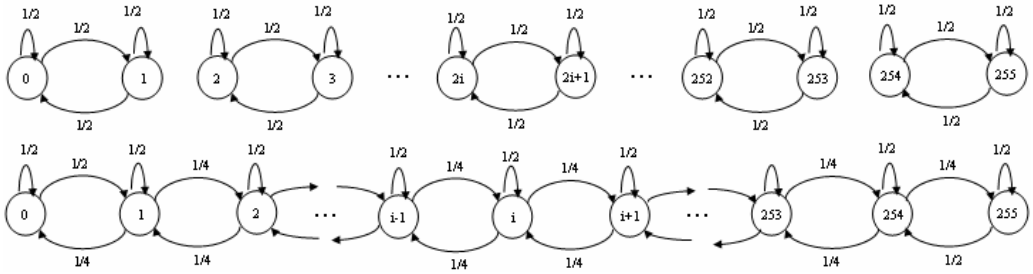
$$h_i=\left|\{(m,n)\mid I(m,n)=i\}\right|$$

در اینجا منظور از h_i، تعداد پیکسل‌های با روشنایی i در تصویر است[11]. فرض کنید برای هیستوگرام تصویر پوشانه و تصویر استگو به ترتیب از نمادهای h_i و h'_i استفاده کنیم. در روش *LSB-M* مقدار h'_i تحت تأثیر سه مقدار h_{i-1}، h_i و h_{i+1} قرار می‌گیرد. به عبارت دیگر، می‌توان گفت

جدول۱: احتمال تغییرات سطح روشنایی پیکسلها

j	i	روش	$P(i\to j\mid d=0)\,P(d=0)+P(i\to j\mid d=1)\,P(d=1)$							$P(i\to j)$
$i-1$	زوج	LSB-F	0	*	1/2	+	0	*	1/2	0
		LSB-M	0	*	1/2	+	1/2	*	1/2	1/4
	فرد	LSB-F	1	*	1/2	+	0	*	1/2	1/2
		LSB-M	1/2	*	1/2	+	0	*	1/2	1/4
i	زوج	LSB-F	1	*	1/2	+	0	*	1/2	1/2
		LSB-M	1	*	1/2	+	0	*	1/2	1/2
	فرد	LSB-F	0	*	1/2	+	1	*	1/2	1/2
		LSB-M	0	*	1/2	+	1	*	1/2	1/2
$i+1$	زوج	LSB-F	0	*	1/2	+	1	*	1/2	1/2
		LSB-M	0	*	1/2	+	½	*	1/2	1/4
	فرد	LSB-F	0	*	1/2	+	0	*	1/2	0
		LSB-M	1/2	*	1/2	+	0	*	1/2	1/4

18 Additive noise
19 Gaussian noise
20 Gray scale images



شکل۳: مدل تغییر مقدار سطح روشنایی یک پیکسل در اثر جاسازی یک بیت داده در روش (الف) *LSB-M* (ب) *LSB-F*

مقدار نهایی h'_i حاصل سه مورد زیر است:

- تعداد پیکسل‌هایی با روشنایی $i-1$ که نویزی با مقدار $+1$ به آن‌ها اضافه شده است.
- تعداد پیکسل‌هایی با روشنایی i که مقدار آن‌ها تغییری نکرده است.
- تعداد پیکسل‌هایی با روشنایی $i+1$ که نویزی با مقدار -1 به آن‌ها اضافه شده است.

می‌توان هر کدام از موارد بالا را با یک توزیع برنولی مدل کرد. مورد اول یک آزمایش برنولی است که h_{i-1} بار تکرار می‌شود و در هر تکرار احتمال موفقیت آن (تبدیل $i-1$ به i) $1/4$ و احتمال شکست (عدم تبدیل $i-1$ به i) $3/4$ است. مورد دوم نیز یک آزمایش برنولی است که h_i بار تکرار می‌شود و در هر تکرار احتمال موفقیت آن (عدم تغییر i) $1/2$ و احتمال شکست (تغییر i) نیز $1/2$ است. مورد سوم نیز توزیعی مانند مورد اول دارد. بنابراین در صورتی که از تمام پیکسل‌های تصویر برای جاسازی استفاده شود، می‌توان متغیر تصادفی توزیع تعداد پیکسل‌های با مقدار i پس از جاسازی، H'_i، را به صورت زیر بیان کرد:

$$H_i' = \sum_{j=1}^{h_{i-1}} S_{+1} + \sum_{j=1}^{h_i} S_0 + \sum_{j=1}^{h_{i+1}} S_{-1}$$

آزمایش برنولی اول، دوم و سوم به ترتیب با نمادهای S_{+1} (اضافه شدن نویزی با مقدار $+1$)، S_0 (اضافه شدن نویزی با مقدار 0) و S_{-1} (اضافه شدن نویزی با مقدار -1) نمایش داده شده‌اند. اگر n آزمایش برنولی مستقل، همگی با احتمال موفقیت p انجام شوند، آنگاه متغیر تصادفی X که تعداد موفقیت‌ها را نشان می‌دهد، متغیری دوجمله‌ای با پارامترهای n و p است. با توجه به مستقل بودن تکرارهای مختلف آزمایش‌های برنولی تعریف شده در بالا، می‌توان متغیرهای دوجمله‌ای مربوطه را تعریف کرد. $M_{+1} = \sum_{j=1}^{h_{i-1}} S_{+1}$ یک متغیر دوجمله‌ای با پارامترهای $n = h_{i-1}$ و $p = 1/4$ است. $M_0 = \sum_{j=1}^{h_i} S_0$ نیز یک متغیر دوجمله‌ای با پارامترهای $n = h_i$ و $p = 1/2$ است. به همین ترتیب $M_{-1} = \sum_{j=1}^{h_{i+1}} S_{-1}$ یک متغیر دوجمله‌ای با پارامترهای $n = h_{i+1}$ و $p = 1/4$ است. بنابراین H'_i مجموع سه متغیر دو جمله‌ای است.

$$H'_i = M_{+1} + M_0 + M_{-1}$$

با توجه به این نکته که در صورت بزرگ بودن مقدار n، می‌توان توزیع دوجمله‌ای با پارامترهای (n, p) را با یک توزیع نرمال با پارامترهای $(np, np(1-p))$ تخمین زد، بنابراین متغیر تصادفی H'_i را می‌توان به صورت زیر نیز تعریف کرد:

$$H'_i = N(h_{i-1}.1/4, h_{i-1}.3/16) + N(h_i.1/2, h_i.1/4) + N(h_{i+1}.1/4, h_{i+1}.3/16)$$

می‌دانیم که توزیع مجموع چند متغیر تصادفی نرمال، یک توزیع نرمال با پارامترهای زیر است:

$$\sum_{i=1}^{n} N(\mu_i, \sigma_i^2) = N(\sum_{i=1}^{n} \mu_i, \sum_{i=1}^{n} \sigma_i^2)$$

بنابراین با توجه به این رابطه، H'_i را می‌توان به صورت یک متغیر نرمال بیان کرد:

$$H'_i = N(\mu_i = \frac{(h_{i-1} + 2h_i + h_{i+1})}{4}, \sigma_i^2 = \frac{(3h_{i-1} + 4h_i + 3h_{i+1})}{16})$$

البته در این رابطه برای i های موجود در مرز استثنائاتی نیز باید در نظر گرفته شود. h_{-1} و h_{256} را صفر فرض می‌کنیم و برای ۱ و ۲۵۴ پارامترهای توزیع به صورت زیر است:

$$H'_1 = N(\mu_1 = \frac{(2h_0 + 2h_1 + h_2)}{4}, \sigma_1^2 = \frac{(4h_0 + 4h_1 + 3h_2)}{16})$$

$$H'_{254} = N(\mu_{254} = \frac{(h_{253} + 2h_{254} + 2h_{255})}{4},$$
$$\sigma^2_{254} = \frac{(3h_{253} + 4h_{254} + 4h_{255})}{16})$$

با در دست داشتن مدلی که تا اینجا برای روش *LSB-M* پیشنهاد کردیم، می‌توان رفتار الگوریتم *LSB-F* را نیز مدل نمود، زیرا *LSB-F* حالتی خاص از الگوریتم عام *LSB-M* می‌باشد.

$$H'_{2i} = Bino(n_i = h_{2i} + h_{2i+1}, p = 1/2)$$
$$H'_{2i+1} = n_i - H_{2i}$$

بعلاوه می‌توان نشان داد که با استفاده از توزیع نرمال نیز مقدار هیستوگرام بعد از جاسازی به روش *LSB-F* دارای توزیع زیر خواهد بود[۱۴]:

$$H'_{2i} = H'_{2i+1} = N(\mu_i = n_i/2, \sigma_i^2 = n_i/4)$$

۴- تخمین تغییرات هیستوگرام *LSB-F* و *LSB-M*

یکی از معیارهای مقایسه روش‌های مختلف پنهان‌نگاری، بررسی تأثیر هر کدام از روش‌ها روی هیستوگرام تصویر پوشانه است. روشی که کمترین تغییر را روی هیستوگرام ایجاد کند، در برابر حملاتی مقاومتر هستند که بر مبنای تغییر هیستوگرام کار می‌کنند. برای بیان عددی از تأثیر هر روش روی هیستوگرام می‌توان معیاری با عنوان خطا تعریف کرد. خطا را مجموع مربعات تفاضل ستون‌های معادل هیستوگرام تصویر پوشانه و تصویر استگو تعریف می‌کنیم:

$$Error = \sum_{i=0}^{255} (h_i - h'_i)^2$$

h_i و h'_i، مقدار ستون i در هیستوگرام تصویر پوشانه و تصویر استگو است. خطای کمتر به معنای تغییر کمتر در هیستوگرام تصویر پوشانه برای بدست آوردن تصویر میزبان نهایی است. مقدار خطا، علاوه بر نوع روش پنهان نگاری به تصویر پوشانه نیز بستگی دارد. بنابراین اگر بتوان قبل از استفاده از یک روش پنهان نگاری خاص، مقدار خطای روش انتخاب شده برای تصویر پوشانه مورد نظر را تخمین زد، آنگاه بهتر می توان در مورد استفاده از آن روش تصمیم گرفت.

با توجه به مدل ارائه شده برای روش *LSB-M* می‌توان تخمینی از خطای این روش را نیز قبل از استفاده از آن محاسبه کرد. امید ریاضی راهی مناسب برای محاسبه مقدار موردانتظار یک متغیر تصادفی است. با توجه به تعریف خطا و با استفاده از قواعد آماری، امید ریاضی خطا را می توان بدین ترتیب محاسبه کرد:

$$E(Error) = E[\sum_{i=0}^{255} (h_i - H'_i)^2] = \sum_{i=0}^{255} E[(h_i - H'_i)^2]$$

پس کافی است بتوان امید ریاضی مربع تفاوت دو ستون معادل از هیستوگرام تصویر پوشانه و استگو را محاسبه کرد. می‌دانیم:

$$E[(h_i - H'_i)^2] = E[h_i^2] + E[H'^2_i] - 2E[h_i H'_i]$$

با توجه به این که h_i، مقدار ستون i در هیستوگرام تصویر پوشانه است و مقدار آن مشخص است، بنابراین h_i به صورت یک ثابت فرض می‌شود و :

$$E[(h_i - H'_i)^2] = h_i^2 + E[H'^2_i] - 2h_i E[H'_i]$$

بنابراین تنها مسئله باقی مانده محاسبه $E[H'_i]$ و $E[H'^2_i]$ است. نشان داده شد که H'_i در جاسازی به روش *LSB-M* حاصل مجموع سه متغیر تصادفی دوجمله‌ای است. برای هر متغیر تصادفی X می‌دانیم که:

$$Mgf_X(t) = E(e^{tx}) \quad , \quad E[X^n] = M_X^{(n)}(0)$$

اگر X یک متغیر تصادفی دوجمله‌ای باشد:

$$Mgf_X(t) = (pe^t + q)^n$$
$$E[X] = np \quad , \quad E[X^2] = np + n(n-1)p^2$$

بنابراین در مورد سه متغیر تصادفی دوجمله‌ای M_{-1}, M_0, M_{+1} می‌وان گفت:

$$Mgf_{M_{+1}}(t) = (1/4\, e^t + 3/4)^{h_{i-1}} \quad , \quad E[M_{+1}] = h_{i-1}/4$$
$$Mgf_{M_0}(t) = (1/2\, e^t + 1/2)^{h_i} \quad , \quad E[M_0] = h_i/2$$
$$Mgf_{M_{-1}}(t) = (1/4\, e^t + 3/4)^{h_{i+1}} \quad , \quad E[M_{-1}] = h_{i+1}/4$$

بعلاوه می‌دانیم:

$$Mgf_{H'_i}(t) = Mgf_{M_{+1}+M_0+M_{-1}}(t) =$$
$$Mgf_{M_{+1}}(t).Mgf_{M_0}(t).Mgf_{M_{-1}}(t)$$

با جاگذاری مقادیر مناسب در این فرمول و استفاده از فرمول‌های قبلی، امیدهای موردنظر بدین صورت محاسبه می‌شوند:

$$E[H'_i] = h_{i-1}/4 + h_i/2 + h_{i+1}/4$$

$$E[H_i'^2] = \frac{(h_{i-1}.(h_{i-1}-1)+4.h_i.(h_i-1)+h_{i+1}(h_{i+1}-1))}{16} + \frac{(2.h_{i-1}.h_i+h_{i-1}.h_{i+1}+2.h_i.h_{i+1})}{8} + \frac{(h_{i-1}+2.h_i+h_{i+1})}{4}$$

انتظار داریم که مقدار نهایی H_i' در واقع مجموع نیمی از مقدار ابتدایی h_i و 1/4 از مقدار ابتدایی h_{i-1} و 1/4 از مقدار ابتدایی h_{i+1} باشد. مشاهده می‌شود که مقدار امید H_i' با مقداری که به روش تحلیلی انتظار داشتیم مساوی شده است. این تساوی می‌تواند تضمینی برای مدل ارائه شده باشد. البته در روابط بالا برای i های موجود در مرز استثنائاتی نیز باید در نظر گرفته شود. با حل شدن مسئله محاسبه $E[H_i']$ و $E[H_i'^2]$، حال می‌توان محاسبه امید خطا را نیز تکمیل کرد.

از طرف دیگر، با توجه به این که H_i' را با یک متغیر تصادفی نرمال نیز مدل کردیم و می‌دانیم:

$$E[H_i'] = \mu_i \quad , \quad E[H_i'^2] = \mu_i^2 + \sigma_i^2$$

بنابراین با حل شدن مسئله محاسبه $E[H_i']$ و $E[H_i'^2]$، حال می‌توان محاسبه امید خطا را نیز تکمیل کرد.

$$E(Error) = \sum_{i=0}^{255} (h_i^2 + E[H_i'^2] - 2h_i E[H_i]) = \sum_{i=0}^{255} (h_i^2 + \mu_i^2 + \sigma_i^2 - 2h_i\mu_i)$$

بنابراین با استفاده از توزیع نرمال نیز می‌توانیم تخمینی از خطای هیستوگرام در روش *LSB-M* محاسبه کنیم.

مشابه محاسبات بالا را می‌توان برای تخمین تغییرات هیستوگرام در روش *LSB-F* نیز تکرار کرد. برای اجتناب از طولانی شدن بحث، تنها به نتایجمدل ریاضی اشاره می‌کنیم. در صورت استفاده از توزیع دوجمله‌ای و با در نظرگرفتن رابطه $n_i = h_{2i} + h_{2i+1}$، روابط زیر برای $E[H_i']$ و $E[H_i'^2]$ برقرار است:

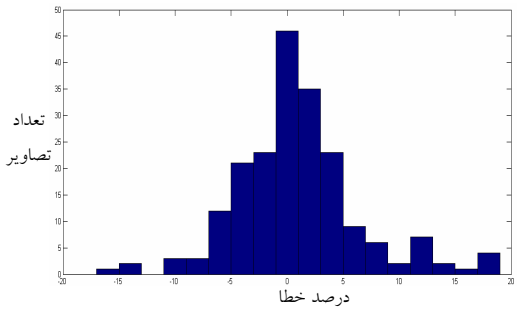
$$E[H'_{2i}] = E[H'_{2i+1}] = n/2$$
$$E[H'_{2i}{}^2] = E[H'_{2i+1}{}^2] = n/2 + n(n-1)/4$$

با استفاده از توزیع نرمال، فرمول محاسبه $E[H_i']$ و $E[H_i'^2]$ در روش *LSB-F* نیز مشابه فرمول محاسبات توزیع نرمال در روش *LSB-M* است. فقط تفاوت در مقدار μ_i و σ_i است، که برای هر دو روش در بخش قبل محاسبه کردیم.

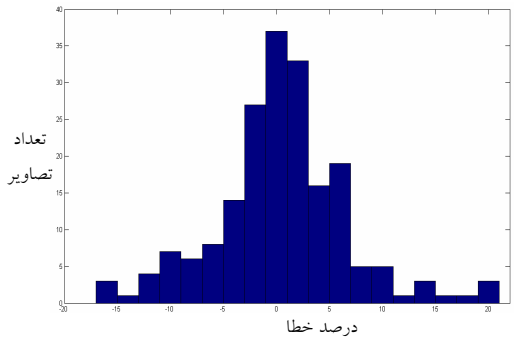
۵- مقایسه نتایج حاصل از تئوری و شبیه‌سازی

برای تست مدل ریاضی ارائه شده، در ۲۰۰ تصویر با استفاده از الگوریتم *LSB-F* و *LSB-M* جاسازی کرده و میزان خطای حاصل از شبیه سازی و خطای حاصل از محاسبات ریاضی را با استفاده از هر دو روش توزیع دوجمله ای و توزیع نرمال محاسبه کردیم. نتایج تخمین خطا با استفاده از هر دو توزیع کاملاً یکسان است. هیستوگرام درصد اختلاف مقدار واقعی و مقدار حاصل از تخمین ریاضی خطا در شکل ٤ و٥ نشان داده شده است.

این شکل دقت بالای تخمین حاصل از مدل ریاضی ارائه شده را نشان می‌دهد. همانگونه که دیده می‌شود در اکثر تصاویر، نتایج شبیه سازی و مدل ریاضی ارائه شده کاملاً مشابه بوده است و اختلاف خطاهای تولید شده برابر با صفر می‌باشد. بعلاوه مقایسه دو نمودار نشان می‌دهد که تخمین تغییرات هیستوگرام در روش *LSB-F* دقیق‌تر از روش *LSB-M* انجام شده است.



شکل۴: هیستوگرام درصد اختلاف شبیه‌سازی و مدل در *LSB-F*



شکل ۵: هیستوگرام درصد اختلاف شبیه‌سازی و مدل در *LSB-M*

۶- نتیجه گیری

بررسی رفتار الگوریتم‌های پنهان‌نگاری به شناسایی هر چه بهتر مزایا و معایب روش‌ها، ارائه حملات موفق و بعلاوه

پیشنهاد روش‌های پنهان‌نگاری مقام‌تر منجر می‌شود. در این مقاله با ارائه یک مدل ریاضی، رفتار الگوریتم‌های پنهان‌نگاری *LSB-M* و *LSB-F* به طور کامل بررسی شده است.

الگوریتم‌های پنهان‌نگاری تغییراتی را در ویژگی‌های تصویر پوشانه ایجاد می‌کنند، که هیستوگرام تصویر یکی از این ویژگی‌ها است. در این مقاله با استفاده از مدل ریاضی ارائه شده برای روش‌های *LSB-M* و *LSB-F*، تخمینی از تغییرات هیستوگرام تصویر ارائه شد. تخمین میزان تغییرات هیستوگرام قبل از جاسازی پیام، می‌تواند مبنایی برای انتخاب تصویری با کمترین تغییر به عنوان تصویر پوشانه باشد. معادل بودن نتایج شبیه‌سازی‌ها و مدل ارائه شده بیانگر صحت فرضیات این مقاله بوده است.

۷- مراجع

[1] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn, "Information Hiding - A Survey", *Proc. of IEEE*, pp.1062-1078, July, 1999.

[2] R.J Anderson and F.A.P. Petitcolas, "On the Limits of Steganography", *IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and privacy Protection*, Vol. 16(4), pp. 474-481, May 1998.

[3] M. M. Amin, M. Salleh, S. Ibrahim, M.R. Katmin and M.Z.I. Shamsuddin," Information Hiding using Steganography", *4th National Conference on Telecommunication Technology Proceedings*, 2003.

[4] B. ŞİMŞEK, "*Steganography in JPEG Images*", Dokuz Eylül University, İZMİR, July, 2004.

[5] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography", *IEEE Security & Privacy*, pp. 32-44, May-June, 2003.

[6] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", *Computer*, Vol. 31, No. 2, pp.26–34, 1998.

[7] Y.K Lee and L.H. Chen, "High capacity image steganographic model," *Vision, Image and Signal Processing, IEE Proceedings*, Vol. 147, Jun 2000.

[8] N. Provos, "Defending Against Statistical Steganalysis", *Proc. 10th Usenix Security Symp, Usenix Assoc.*, pp. 323-335, 2001.

[9] A. Westfeld, "F5-A Steganographic Algorithm :High Capacity Despite Better Steganalysis", *Proc. 4th Int'l Information Hiding Workshop, Springer-Verlog*, Vol. 2137 , Berlin Heidelberg New York , pp.289-302, 2001.

[10] A. Westfeld and A. Pfitzman, "Attacks on Steganographic Systems", *Proc. 3rd Int'l Information Hiding Workshop , Springer-Verlag*, Berlin Heidelberg New York, pp. 61-76, 1999.

[11] A. D. Ker, "Steganalysis of LSB Matching in Grayscale Images", *IEEE Signal Processing Letters*, Vol. 12, No. 6, June 2005.

[12] A. Westfeld, "Detecting low embedding rates," *in Proc. Inf. Hiding Workshop, Springer LNCS*, vol. 2578, 2002.

[13] J. Fridrich, , M. Goljan, and R. Du, "Reliable Detection of LSB Steganography in Grayscale and Color Images", *Proc. of ACM: Special Session on Multimedia Security and Watermarking*, pp. 27-30, Ottawa, Canada, 2001.

[14] مهدوی، م.، سماوی، ش.، ذاکر، ا. ، منصوری، ف. ، "روشی جدید مبتنی بر گرادیان محلی هیستوگرام تصویر برای پنهان شکنی در استگانوگرافی"، *دوازدهمین کنفرانس بین المللی کامپیوتر*- تهران- اسفند ۱۳۸۵

[15] A. Ker, "Improved detection of LSB steganography in grayscale images, *in Proc. Inf. Hiding Workshop, Springer LNCS*, vol. 3200, 2004.

[16] مهدوی، م. ، سماوی، ش.، اخوت، م. ، اکرمی، ص. ، "روش پنهان نگاری تطبیقی بر اساس اغتشاش جمع شونده"، *پانزدهمین کنفرانس مهندسی برق ایران*، اردیبهشت ۱۳۸۶