سازی داده ها انجام می شود. تقریباً در همه موارد داده ها قبل از آنکه ذخیره شوند یا انتقال داده شوند فشرده می گردند این بدلیل حجم داده های تصویری و اضافات بسیار زیاد آنهاست بنابراین آمیختن نیازهای امنیتی با سیستمهای فشرده سازی داده اهمیت بسیار دارد. مشکل اساسی این است که چگونه در حالی که هزینه محاسبات را بدون کاهش کیفیت عملکرد فشرده سازی کاهش می دهیم از امنیت مناسب نیز اطمینان حاصل کنیم. ه- تغییر تصویر به صورتی که قابلیت هیچگونه تشخیصی وجود نباشد: بینایی انسان نسبت به نویز و تخریب جزئی تصویر مقاومت زیادی دارد و برای محافظت از تصویر باید بیت هایی که با هم همبستگی زیادی دارند بخوبی رمز گردند. در صورتی که در روشهای سنتی رمزنگاری به همه بیتهای داده به شکل یکسانی نگریسته می شود و پس از رمز شدن هم این شباهتها تا حدودی آشکار باقی می مانند بنابراین لازم است که توان محاسباتی زیادی برای رمزنگاری همه بیتهای تصویر صرف شود که اغلب اوقات این حجم محاسبات غیر ضروری است.

فصل ۲

الگوریتم رمزنگاری تصویر مبتنی بر توابع آشوب چی بی شف و تحلیل و بهبود آن

۱.۲ مقدمه

نیاز به رمزنگاری تصویر برای ایجاد انتقال ایمن تصاویر بر روی شبکه اینترنت و شبکه های مخابرات بی سیم بیش از پیش افزایش می یابد ولیکن با توجه به حجم زیاد داده های تصویری و ویدئویی به نظر می رسد الگوریتم های کلاسیکی مانند DES، AES و IDEA از کارایی لازم در این زمینه برخوردار نیستند. خصوصاً در کاربردهای بلادرنگ تصویر مثل ویدئو کنفرانس این روشها با توجه به سرعت بسیار کمشان مناسب به نظر نمی رسند. دومین مشکلی که این الگوریتمها دارند طول کلید آنهاست که با توجه به حجم داده های رمزشده استفاده از کلیدهای با طول محدود باعث ضربه پذیری روش در برابر حملات متن رمزشده می گردد. راه حل های گوناگونی در این رابطه برای افزایش سرعت و امنیت الگوریتمهای رمزنگاری تصویر ارائه شده است. [۱،۲ و ۳] در این بین یکی از روشهایی که بسیار مورد توجه واقع شده، الگوریتم های آشوبگون است. بر خلاف اکثر روش های کلاسیک، الگوریتم هایی که بر مبنای سیستم های آشوب طرح می شوند، روش کاملاً متفاوتی را برای حل این مشکلات ارائه می کنند. این الگوریتم ها اغلب بسیار ساده بوده و هزینه های محاسباتی کمی دارند ولی برای رمز نمودن تصاویر به شکل مناسب بر ویژگی حساسیت آشوب نسبت به مقدار اولیه و پارامتر های سیستم و خواص تصادفی خوب اینگونه سیستم ها تکیه دارند. در نتیجه سادگی این الگوریتم ها، سرعت اجرای آنها بسیار بیشتر است. در روش بلوکی، در چنین الگوریتم هایی می توان با کنترل اندازه بلوکها و تعداد تکرارها بین سرعت اجرا، حساسیت و دقت

الگوریتم شرایط مناسبی را برگزید. در انتها باید گفت که علاوه بر سرعت زیاد، این روش نسبت به تغییراتی بسیار کوچک در کلید بسیار حساس بوده حتی با در دست داشتن مقادیر تقریبی کلید امکان شکستن رمز برای حمله گران وجود ندارد. در این فصل سعی بر این بوده که با استفاده از ویژگیهای توابع آشوب و امکان تولید کلیدهایی با خواص تصادفی بسیار خوب و فضای بزرگ، الگوریتمی ساده، سریع و ایمن برای رمزنگاری داده های تصویری ایجاد شود. ویژگی مهمی که باعث شده آشوبناکی برای رمزنگاری بسیار مورد توجه قرار بگیرد تعریف پذیری سیستم در عین رفتار شبه تصادفی آن است که باعث می گردد خروجی سیستم از دید حمله گران تصادفی به نظر برسد در حالی که از دید گشاینده رمز، سیستمی تعریف پذیر بوده و لذا قابل رمزگشایی است. الگوریتم های رمزنگاری بسیاری بر اساس تئوری آشوب طرح شده اند [۵،۴،۶ و ۷].

پارِک و همکاران در سال ۲۰۰۶ یک الگوریتم رمزنگاری تصویر بر اساس نگاشت آشوب یک بعدی، ارائه دادند[۵]. با این وجود، استفاده از یک نگاشت آشوب برای رمزنگاری تصویر، ممکن است منجر به تولید فضای کلید کوچکتر و در نتیجه امنیت پایین تر شود. بنابراین تعدادی روش جدید برای توسعه طرح های کارآمد رمزنگاری تصویر پیشنهاد شد.

لیان از سیستم آشوب فضایی و زمانی برای رمزنگاری تصویر استفاده کرد و امنیت الگوریتم را به تفصیل، با جزئیات، تجزیه و تحلیل نمود و سازگاری خوب بین امنیت و بازدهی الگوریتم را نشان داد[۶.]

اگر چه این الگوریتم ها دارای فضای کلید بزرگ و میزان حساسیت بالا به مقادیر کلید بودند، ولی امنیت آنها به اندازه کافی بالا نبود. به تازگی بیشتر توجهات به سیستم های فرا–آشوب که دارای حداقل دو نمای لیانوف مثبت، فضای کلید بزرگتر، میزان حساسیت بیشتر و مشخصات دینامیکی پیچیده تر است، جلب شده که شاید مطالعه کاربردهای سیستم های فرا–آشوب در الگوریتم های رمزنگاری تصویر ارزشمند تر باشد]۷[.

فِردریک [۸] فرآیندی از رمزنگاری تصویر که دارای امنیتی است که با تکرار عملیات جانشانی و انتشار برای بیش از یک راند، افزایش می یابد، ارائه داد. بعد ها بسیاری دیگر این عقیده را به خوبی اجرا کردند[۹,۱۰,۱۱,۱۲,۱۳].

۲.۲ تابع آشوب چی بی شف

یک چند جمله ای از درجه k–ام چی بی شف به صورت زیر تعریف می شود:

$$T_k(x) = cos(k(\arccos(x)))$$

جایی که $k = ۱, ۲, ۳, ...$ و $x \in [-۱, ۱]$.