مروری بر مقالات درمورد تکنیک های رمزگذاری تصویر

چکیده

رمزگذاری عکس نقش مهمی در تضمین انتقال طبقه بندی شده و ظرفیت عکس در وب بازی می کند. پس از رمزگذاری در زمان مناسب، عکس تحت آزمون مهمی قرار می گیرد زیرا هر عکس شامل اطلاعات اندازه گیری شده ی گسترده ایی است. این مقاله به بررسی رمزگذاری عکس در فضا و در محدوده های فرکانس و هیبریدی- با در نظر گرفتن هر دو استراتژی رمزگذاری کامل و رمز گذاری انتخابی- می پردازد.

کلمات کلیدی: رمزگذاری عکس، محدوده های رمزگذاری عکس، روش های رمز گذاری انتخابی و کامل عکس

1. مقدمه

رمزنگاری در مورد مکاتبات در منطقه ی دشمن است و مسائل مختلف مثل رمزگذاری ، بررسی و تخصیص کلید به صورت یک زوج را شامل می شود. زمینه ی رمزنگاری فعلی مبتی بر یک تئوری اصولی است که براساس آن می توان این مسائل را درک کرد. رمزنگاری بهترین روش برای ارزیابی سنت هاست است، به این صورت که آن ها را استنباط می کند و به چگونگی ایجاد سنت هایی که می توان به آن ها اعتقاد داشت، می پردازد.

داده های رسانه ایی که به طور اتواتیک توسعه یافته اند،به صورت گسترده در دسترس هستند. اخیرا، تجهیز رسانه در عمل و در جهت امنیت مربوط به داده ی صوتی و تصویری ضرورت یافته است و نگرانی هایی در مورد استاندارد این تجهیز وجود دارد. شناسایی مسائل اساسی پیرامون موضوع رمزگذاری انجام شده و بیشتر روی استراتژی های رمزگذاری عکس و نظارت روی مکاتبات حاضر با استفاده از روش های آشوبی تمرکزشده است.

رمزگذاری عکس آشوبی می تواند به وسیله ی ویژگی های آشوبی شامل المان های قطعی، رفتار نامنظم و ایجاد تغییرات غیر مستقیم ساخته شود. با این استدلال، در مسائل معمولی ضمن داشتن محدودیت های امنیتی، بررسی های دیداری تسریع می شود، که این موضوع ممکن است در یک زوج از درخواست ها مناسب باشد.

تصاویر خودکار بزرگترین بخش مورد استفاده به عنوان بخشی از دستورهای گوناگون که ارتش را نظم می دهد، چهارچوب های کاری مفید و حقیقی هستند که دسترسی به آن ها باید به صورت کنترل شده انجام شود. این چهارچوب ها ابزارهایی برای اثبات درست بودن عکس ها ارائه می دهند.

قدیمی ترین و مهم ترین مسئله در رمزنگاری، ایمنی ارتباط در یک کانال ضعیف است. بخش A باید به بخش B یک پیام رمز در طول خط مکاتبات بفرستد، که ممکن است به وسیله ی دشمن دریافت شود. پیشرفت های اخیر در مهندسی به ویژه در صنعت خودرو و مکاتبات، اجازه ی تجارت های بزرگ جهت مناسب سازی محاسبات انجام شده برای محتوای رسانه از طریق اینترنت را صادر کرد.

پس از آن با افزایش آرشیوهای پیشرفته ، لوازم بررسی عکس و قابلیت دسترس در اینترنت، شرایط برای کپی رایت در داده های رسانه ایی مثل عکس، محتوا، صدا و ویژگی های محتوایی فراهم شد.

در حال حاضر یک آزمون متناوب جهت ایمن سازی روش های جدید- که دارای مجوز باشند- در سیستم های صوتی و تصویری انجام می شود.

برای مدیریت مسائل خاص، دو پیشرفت چشمگیر جهت ایجاد امنیت در عکس ها حاصل شده است که عبارتند از: آ) استفاده از روش های رمز گذاری عکس که امنیت کاملی ایجاد می کند، وقتی از مفاهیم پیشرفته در تعدادی از سیستم های پخش استفاده می شود و ب)استفاده از سیستم های چاپ سفید به عنوان ابزاری در جهت بیمه کردن در برابر کپی رایت ، برخورداری از حق مالکیت و بازبینی. در این مقاله ، به طور جدی روی روش های رمز گذاری تصویر در نقشه های آشوبی آزمایش شده تمرکز شده است.

امنیت رسانه به عنوان قانونی جهت تامین امنیت داده های صوتی و تصویری با استفاده از یک سیستم یا یک مجموعه از روش های مورد استفاده مطرح می شود. این سیستم ها عمدتا روی رمزنگاری متمرکز هستند و هر نوع امنیت مربوط به مکاتبات ، یا امنیت در برابر دستبرد(مدیریت حقوق دیجیتال و واترمارکینگ) یا هر دو را تقویت می کنند.

امنیت مکاتبات عکس های کامپیوتری و متون رسانه ایی پیشرفته می تواند با استفاده از روشی برای رمزنگاری کلیدی متقارن استاندارد تامین شود. این رسانه می تواند به گروه های موازی مرتبط باشد. ممکن است همه ی اطلاعات برای رمزنگاری با استفاده از استانداردهایی مثل استاندارد رمزگذاری پیشرفته (AES) و استاندارد رمزگذاری داده (DE)، کدگذاری شوند. به عنوان یک قانون، وقتی اطلاعات در محیط، ساکن باشند (جریان پیوسته نیست)، می توانند به عنوان اطلاعات دوتایی استاندارد مورد استفاده قرار گیرند و روش های رمزگذاری ممکن روی آن ها اجرا شود. برای رسیدن به سطح امنیت ایده آل، حفاظت از داده ی صوتی و تصویری از طریق تخصیص اجباری بیمه به آن انجام می شود. در حال حاضر محاسبات زیادی برای رمزگذاری عکس در دسترس می باشد، مثل نقشه ی آرنولد، الگوریتم تانگرام، انتقال بیکر، انتقال مرجع سه بعدی جادویی، انتقال نسبی و...

در تعداد کمی از محاسبات، کلید رمز و محاسبات نمی توانند متفاوت باشند. در این موارد شرایط لازم برای رمزنگاری فراهم نمی شود و فایل هایی که از این طریق رمزگذاری شده اند مستعد قرار گرفتن تحت حملات متفاوت هستند. اخیرا، از روش های رمزگذاری عکس که در رفرنس های 2 و 3 و 10-8 بیان شده است، استفاده می شود تا بر چنین معایبی غلبه شود.

این مقاله به صورت زیر سازمان دهی شده است : در قسمت2، در مورد مقدمات رمزنویسی بحث کردیم. در قسمت 3 مروری بر مقالات مشتمل بر روش های رمزنگاری عکس مبتنی بر الگوریتم های کامل و انتخاب شده بحث می کنیم. به علاوه دسته بندی طرح های رمزگذاری تصویر در سه محدوده را ارائه داده ایم. نتایج هم در آخرین بخش ارائه شده است.

2. مقدمات

2.1. متن ساده

پیام اصلی شخصی جهت ایجاد ارتباط با دیگران به عنوان متن ساده تعریف شده است. در رمزنگاری یک پیام که در نهایت به دیگران فرستاده می شود،متن ساده نام دارد.

2.2. متن رمزی

پیامی که به وسیله ی هرکس فهمیده نمی شود یا پیامی که برای ما بی معناست، پیام رمزی نامیده می شود. در رمزنگاری پیام اصلی قبل از انتقال پیام به پیام غیر قابل خواندن تبدیل می شود.

2.2.1. رمزها

یک رمز یک متن منفرد یا گروهی از متن ها را به صورت واحد و صرف نظر از مفهوم،رمزگذاری می کند.

2.2.2. کدها

یک کد به طور معمول یک کلمه یا عبارت را در یک زمان و با یک روش ثابت (بدون کلیدها) کدگذاری می کند.

2.3. رمزگذاری

فرآیند تبدیل یک متن ساده به متن رمزی، رمزگذاری نامیده می شوود. رمزنگاری از روش های رمزگذاری استفاده می کند تا پیام های محرمانه را از طریق یک کانال ناامن بفرستد. فرآیند رمزگذاری نیاز به دو چیز دارد: یک الگوریتم رمزگذاری و یک کلید. الگوریتم رمزگذاری به معنای تکنیک هایی است که در رمزگذاری مورد استفاده قرار می گیرد. رمزگذاری در طرف فرستنده انجام می شود.

2.4. رمزگشایی

فرآیند معکوس رمزگذاری، رمزگشایی نامیده می شود و فرآیند تبدیل متن رمزدار به متن ساده است. رمزنگاری روش های رمزگشایی را در طرف دریافت کننده به کار می برد تا پیام اصلی را از پیام غیر قابل خواندن (پیام رمزی) استخراج کند. فرآیند رمزگشایی نیاز به دو چیز دارد: یک الگوریتم رمزگشایی و یک کلید. الگوریتم رمزگشایی به معنای روش هایی است که در رمزگشایی مورد استفاده قرا می گیرد. عمدتا الگوریتم های رمزگذاری و رمزگشایی یکسان هستند.

2.5. کلید

کلید یک عدد یا یک متن عدد آلفا یا ممکن است یک نماد خاص باشد. کلید زمانی که رمزگذاری در متن ساده انجام می شود و زمانی که رمزگشایی در متن رمزی اتفاق می افتد، استفاده می شود. انتخاب کلید در رمزنگاری بسیار مهم است زیرا امنیت الگوریتم رمزگذاری بستگی به آن دارد.

2.6. هدف از رمز نگاری

رمزنگاری تعدادی اهداف امنیتی جهت محافظت از داده ی شخصی ، داده ی بدون تغییر و غیره فرام می کند. به دلیل مزایای بزرگ رمزنگاری در داشتن امنیت امروزه به طور گسترده از آن استفاده می شود. در ادامه اهداف مختلف رمزنگاری آورده شده است.

2.6.1. محرمانه بودن

اطلاعات در کامپیوتر منتقل می شود و فقط باید به وسیه ی مالک آن و نه هیچ کس دیگری قابل دسترسی باشند.

2.6.2. تایید کردن

اطلاعات دریافت شده به وسیله ی هر سیستم باید بررسی شود تا فرستنده را شناسایی کند که آیا اطلاعات از شخص مورد نظر فرستاده شده اند یا نادرست و قلابی هستند.

2.6.3. امانت داری

فقط مالک اجازه داد تا اطلاعات انتقالی را اصلاح کند. هیچ کس بین فرستنده و دریافت کننده اجازه ندارد پیام داده شده را اصلاح کند.

2.6.4. انکارناپذیربودن

انتقال پیام به صورتی است که نه فرستنده و نه دریافت کننده ی پیام قادر نیستند انتقال پیام را انکار کنند.

2.6.5. کنترل دسترسی

فقط اشخاص صاحب اختیار قادر هستند تا به اطلاعات داده شده دسترسی داشته باشند.

2.7. دسته بندی رمزنگاری

الگوریتم های رمزگذاری می توانند به دو دسته ی وسیع رمزگذاری کلیدی متقارن و نامتقارن تقسیم بندی شوند.

2.7.1. رمزگذاری متقارن

در رمزگذاری متقارن کلید مورد استفاده برای رمزگذاری شبیه به کلید مورد استفاده در رمزگشایی است. بنابراین توزیع کلید باید پیش از انتقال اطلاعات انجام شود. کلید نقش بسیار مهمی در رمزنگاری متقارن بازی می کند زیرا امنیت رمزنگاری به طور مستقیم وابسته به ماهیت کلید مثل طول کلید و غیره است. الگوریتم های کلیدی متقارن

متفاوتی وجود دارد مثل DES، TRIPLE DES ،AES، RC4، RC6 و BLOWFISH. الگوریتم های متقارن دو نوع هستند:

2.7.1.1. رمزهای قفل

2.7.1.2. رمزهای رشته

2.7.1.1. رمزهای قفل: رمز قفل تابعی است که قفل های متن ساده ی n بیتی را به قفل های متن رمزی نظیر می کند، nطول قفل است و ممکن است به صورت یک رمز جانشینی ساده با کاراکتر بزرگ مشاهده شود. تابع به وسیله ی کلید k (k بیتی) پارامتریک شده است و مقادیر را از زیر مجموعه ی k (فضای کلید) دریافت می کند تا بردارهایk بیتی v_k را ایجاد کند. عمدتا فرض می شود که انتخاب کلید تصادفی است. استفاده از قفل های متن ساده و متن رمزی با اندازه ی یکسان از گسترش داده جلوگیری می کند.

2.7.1.1.2. تعریف: یک رمز قفل n بیتی تابع $E{:}V_n \times K \rightarrow V_n$ است که برای هر کلید $\mathbb{K} \in K$ است و $E(P;\mathbb{K})$ یک نقشه با قابلیت معکوس کردن (تابع رمزگذاری برای$\mathbb{K}$) از v_n تا v_n است که به صورت $E_{\mathbb{K}}(P)$ نوشته می شود. نقشه ی معکوس، تابع رمزگشایی است و به وسیله ی $D_{\mathbb{K}}(C)$ مشخص می شود. $C = E_{\mathbb{K}}(P)$ مشخص می کند که متن رمزی C از رمزگذاری متن ساده ی P تحت k نتیجه شده است.

2.7.1.1.3. تعریف: یک رمز تصادفی یک رمز قفل n بیتی است که 2^n بار اجرا می شود! به صورت یک به یک در 2^n المان. هر 2^n کلید به یک استحاله اختصاص دارد.

2.7.1.2. رمزهای رشته ایی: رمزهای رشته ایی یک گروه مهم از الگوریتم های رمزگذاری است که کاراکترهای منفرد پیام متنی ساده را با استفاده از انتقال رمزگذاری که با زمان تغییر می کند، در یک زمان رمزگذاری می کنند. رمزهای رشته ایی عمدتا سریعتر از رمزهای قفل در سخت افزار هستند و پیچیدگی کمتری در مدارات سخت افزار دارند.

علاوه براین،استفاده از آن ها وقتی در هم آمیختگی محدود است یا وقتی کاراکترها به محض اینکه دریافت می شوند باید جداگانه پردازش شوند، مناسب تر بوده و در بعضی موارد استفاده از آن ها اجباری است (برای مثال در بعضی اپلیکیشن های ارتباط راه دور). از آن جا که رمزهای رشته ایی در انتشار خطا محدودیت دارند ، ممکن است در مواقعی که احتمال انتقال خطا بالاست،سودمند باشند. رمزهای رشته ایی به طور رایج به دو نوع سنکرون و خود سنکرون تقسیم بندی می شوند.

2.7.1.2.1. رمزهای رشته ایی سنکرون:رمز رشته ایی سنکرون یک رشته ی کلیدی است که مستقل از پیام متنی ساده و از متن رمزی تولید می شود. فرآیند رمزگذاری یک رمز رشته ایی سنکرون می تواند به وسیله ی معادلات زیر توصیف شود:

$$\begin{aligned} \beta_{i+1} &= f(\beta_i, K), \\ \alpha_i &= g(\beta_i, K)\ , \\ c_i &= h(\alpha_i, m_i), \end{aligned} \qquad (2.1)$$

که β_0 حالت اولیه است و ممکن است از کلید k تعیین شود، f تابع حالت بعدی است،g تابعی است که رشته کلیدی α را تولید می کند و h خروجی تابعی است که رشته ی کلیدی و متن ساده ی m را در هم می آمیزد تا متن رمزی C تولید شود.

2.7.1.2.2. رمزهای رشته ایی خود سنکرون: رمز رشته ایی خود سنکرون یا ناهمگام یک رشته ی کلیدی است که به عنوان تابع کلید و اعداد ثابت از رقم های متن رمزی قبلی ایجاد می شود. تابع رمزگذاری مربوط به یک رمز رشته ایی خود سنکرون می تواند به وسیله ی معادلات زیر توصیف شود:

$$\begin{aligned}\beta &= (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1}),\\ \alpha &= f(\beta_i, K)\ ,\\ c_i &= g(\alpha_i, m_i),\end{aligned} \qquad (2.2)$$

که $\beta_0 = (c_{-t},\ c_{-t+1},\ \ldots,\ c_{-1})$ حالت اولیه (بدون رمز) است ،k کلید است، f تابعی است که رشته ی کلیدی α را تولید می کند و g خروجی تابعی است که رشته ی کلید و متن ساده ی m را ترکیب می کند تا متن رمزی C تولید شود.

2.7.2. رمزگذاری نامتقارن

رمز نگاری نامتقارن یا رمزنگاری کلید عمومی، رمزنگاری است که در آن از یک جفت کلید برای رمزگذاری و رمزگشایی یک پیام استفاده می شود تا پیام به سطح ایمنی مورد نظر برسد. در ابتدا، کاربر شبکه یک جفت کلید عمومی و خصوصی از اشخاص معتبر دریافت می کند. هر کاربر دیگری که بخواهد یک پیام رمزگذاری شده بفرستد می تواند یک کلید عمومی دریافت کند. فرستنده از این کلید استفاده می کند تا پیام را رمزگذاری کند و پیام را به دریافت کننده می فرستد. وقتی دریافت کننده پیام را دریافت می کند، آن را با کلید خصوصی خودش که هیچ کس دیگری به آن دسترسی ندارد،رمزگشایی می کند.

2.8. انتشار و در هم ریختگی

شانُن در یکی از مقالات بنیادین در اصول تئوری رمزگذاری ، دو یژگی که یک رمزنگاری خوب باید داشته باشد تا آنالیزهای آماری را به تاخیر بیندازد ارائه داد: انتشار و در هم ریختگی. انتشار به این معناست که اگر یک ویژگی متن

ساده را تغییر دهیم ، باید چندین ویژگی متن رمزی تغییر کند و به طور مشابه اگر یک ویژگی متن رمزی را تغییر دهیم، چندین ویژگی از متن ساده باید تغییر کند. این مطلب به این معناست که فرکانس های آماری از نامه ها در متن ساده ، در طول چندین ویزگی در متن رمزی منتشر می شوند، که به این معناست که متن رمزی خیلی بیشتری نیاز است تا یک متن معنادار ایجاد شود. انتشار به این معناست که کلید با یک روش ساده به متن رمزی مرتبط نیست. به ویژه، هر کاراکتر از متن رمزی باید وابسته به چندین بخش از یک کلید باشد.

2.9. فضا و محدوده ی فرکانس

2.9.1. محدوده ی فضایی

در روش محدوده ی فضایی، پیکسل ساخته شده از جزئیات تصویر در نظر گرفته می شود و روش های مختلف مستقیما به این پیکسل ها اعمال می شود. توابع پردازش عکس در محدوده ی فضایی ممکن است به صورت زیر بیان شوند:

$$g(x,y) = T[f(x, y)] \qquad (2.3)$$

که f(x,y) عکس ورودی،g(x.y) عکس خروجی پردازش شده است و T عملکرد f تعریف شده در مجاورت (x,y) را نشان می دهد. گاهی اوقات T هم چنین می تواند برای عمل کردن در یک مجموعه از تصاویر ورودری به کار رود. قلمرو فضایی، فضای تصویر نرمال است که در آن یک تغییر در موقعیت در عکس I به طور مستقیم منجر به تغییری در موقعیت مرحله ی S می شود. فاصله ها در I (در پیکسل ها) مربوط به فواصل واقعی (برای مثال درm) در S است . علاوه براین می توانیم مشاهده کنیم که فرکانس مقادیر عکس تغییر می کند. این مطلب اینگونه معنا می شود که پیکسل های زیادی یک پیکسل تکراری را به صورت دوره ایی اجرا کنند تا تغییرات شدیدی رخ دهد. این رخداد می تواند مربوط به تعداد پیکسل هایی باشد که یک الگو را در محدوده ی فضایی تکرار می کنند.

2.9.2. محدوده ی فرکانس

محدوده ی فرکانس فضایی است که برای هر عکس در موقعیت F یک مقدار تخصیص می دهد که مقادیر زیادی در تصویر I در طول یک فاصله ی خاص مرتبط با F تغییر می کند. در محدوده ی فرکانس، تغییرات در موقعیت عکس متناظر با تغییرات در فرکانس فضایی است،(یا نرخ مقادیر شدت عکس). در محدوده ی فضایی ساده، ما به طور مستقیم با یک عکس درهم امیخته (مخلوط)سر و کار داریم ، در حالی که در محدوده ی فرکانس ، با عکس ساده سر و کار داریم.

2.9.2.1. مولفه های فرکانس

هرعکس در محدوده ی فضایی می تواند در یک محدوده فرکانس ارائه شود. اما ببینیم این فرکانس ها دقیقا چه کاری انجام می دهند . مولفه های فرکانس را به دو مولفه ی بزرگ تقسیم خواهیم کرد.

2.9.2.2. مولفه های فرکانس بالا

مولفه های فرکانس بالا مرتبط با لبه های عکس است.

2.9.2.3 مولفه های فرکانس پایین

مولفه های فرکانس پایین در عکس مرتبط با بخش های صاف است.

2.9.3 تفاوت بین محدوده ی فضایی و محدوده فرکانس

در محدوده ی فضایی، ما با عکس ها به همان صورتی که هستند سر و کار داریم. مقادیر پیکسل های عکس با ملاحظه به صحنه تغییر می کند، در حالی که در محدوده ی فرکانس مقادیر پیکسل ها در محدوده ی فضایی در حال تغییر هستند.

3. مروری بر مقالات پیرامون روش های رمزگذاری عکس

در این بخش، یک زوج از استراتژی های رمزگذاری عکس که اخیرا پیشنهاد شده اند، ارائه شده است که از نقشه های آشوبی استفاده می کنند تا ماهیت چندعاملی الگوریتم را بالا برده و کلید قوی تری بسازند. در ابتدا روش های رمزگذاری عکس با تمرکز بر طرح های آشوبی در محدوده ی فضایی بیان می شود، در حالی که بخش پایانی مروری بر مقالات سطح مجدد است.

3.1. رمزگذاری کامل

اطلاعات شخصی بخش ضروری رمزگذاری عکس است. سّری بودن داده ی رمزگذاری شده و تعادل در زمان و هزینه ی تولید روش رمزگذاری چالشی است که رمزگذاری هنوز با آن روبه روست. این چالش ها در شماری از گراف های کاری فضایی، محدوده های فرکانس و هیبریدی در طرح رمزگذاری به طور کامل بررسی شده است. در بخش نتیجه گیری، ما روی این روش ها،محدوده های اجرای آن ها و روش های رمزگذاری مثل رمز قفل و رمز رشته ایی با استفاده از یک آزمون، تمرکز خواهیم کرد.

3.1.1. محدوده ی فضایی

در سال 1989، "ماتیوس و روبرت" الگوریتم های رمزگذاری جدیدی ارائه دادند که از سیستم های آشوبی و با بهره گیری از ویژگی های بحرانی سیستم های آشوبی مثل اعتمادسازی در شرایط آغازین و هسته ی پزدو-رندوم که بعد از زمان های معین از رمزگذاری آشوبی تکراری پیش بینی آن ها به سختی انجام می شود، تعیین شدند.

هابوستا و همکارانش کلید رمز یک روش رمزنگاری را به وسیله ی تکرار یک سیستم آشوبی ارائه کردند. در نقشه ی ارائه شده ی آن ها از نقشه ی tent به عنوان نقشه ی آشوبی استفاده شد تا روی اندازه های پارامتر متمرکز شده و از حملات آماری به وسیله ی تست مربع چی ممانعت شود. نتیجه این پزوهش نشان داد که اگر اندازه ی کلید و اندازه ی متن معمولی هر دو در چهارچوب پیشنهاد شده 20 رقم باشند زمان های نقشه کشی باید بزرگتر از 73 باشد. یک

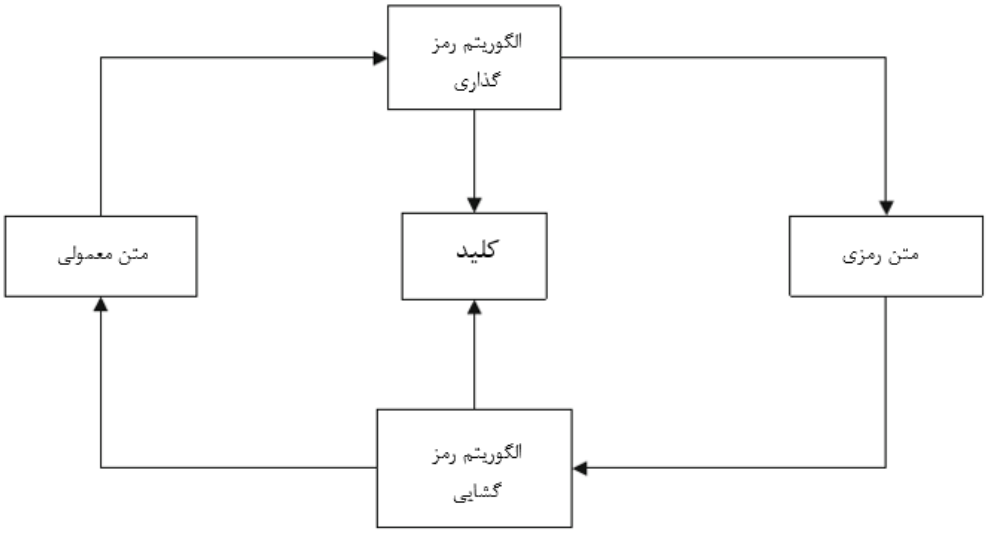
متن معمولی 2n متن رمزی دارد و یکی از 2n متن رمزی به دریافت کننده فرستاده می شود. با در نظر گرفتن این حقیقت که متن رمزی به وسیله ی هر دو روش خود- اظهاری برداشته می شود، دریافت کننده می تواند یک متن ساده فقط با به کار بردن کلید رمز به دست آورد.

"اسچوارتز" یک استراتژی بازچینی برای رمزگذاری عکس ارائه داد. اولین مرحله ی آن تولید یک گروه از نقاط تصادفی در تصویر اصلی است. این نقاط تصادفی به طور موثری به وسیله ی اساس ژنراتور عدد نامنظم کنترل می شود، مبنای این روش، وجود کلید خصوصی در این استراتژی است. سپس این استراتژی برخی خطوط گرافیکی بین هر دو پیشنهاد پیوسته این سکوئنس رسم می کند. به علاوه ، مداد جذب کننده ی آن یک حالت معکوس است که هر سیکل سفید را به سیاه تغییر می دهد. با تقلید از خطوط متضاد زیاد رسم شده در تصویر اصلی ، در نتیجه ی رمزگذاری تصویر ساده حاصل می شود.

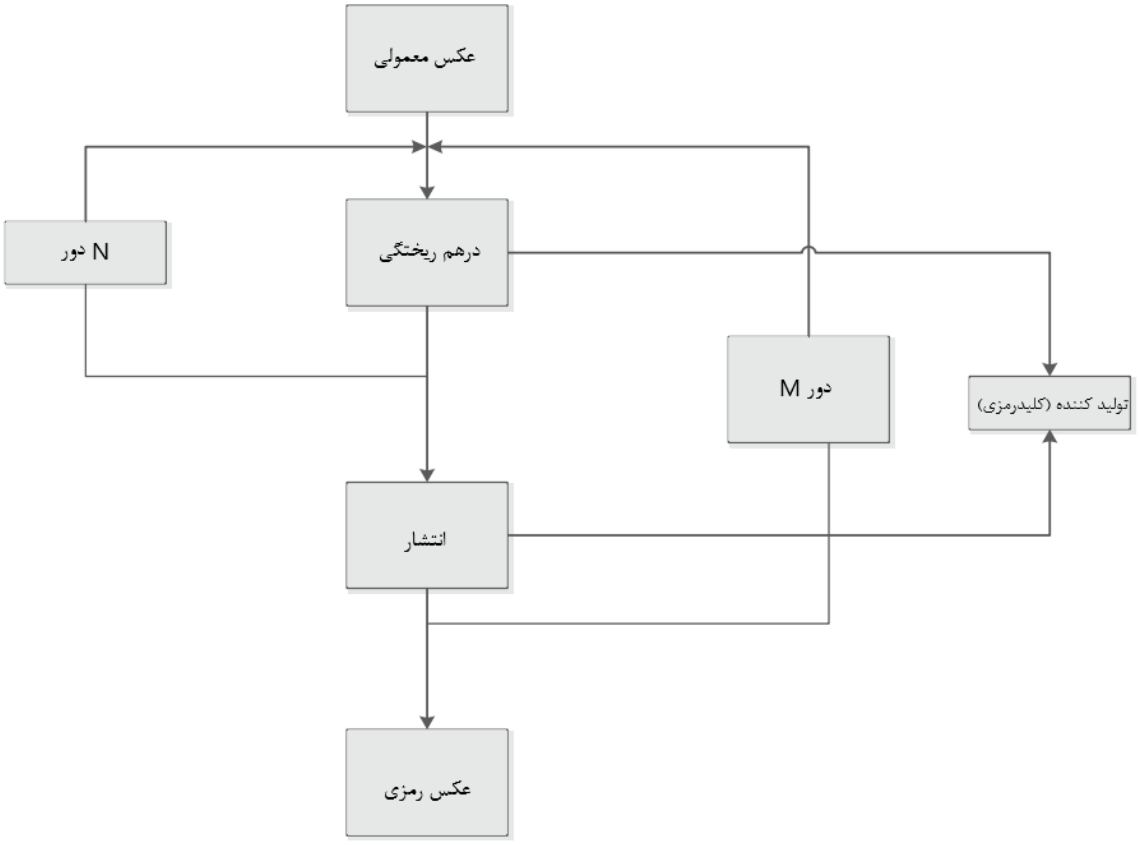
"بوربکیس و آلکسپولز" یک سیستم رمز گذاری عکس متناوب پیشنهاد کردند. در سیستم آن ها طول تصویر 2D به لیست 1D تغییر می کند و از زبان SCAN استفاده می شود تا نتایج رسم شود. در این زبان، تعدادی کمی حروف وجود دارد. هر حرف زبان SCAN با یک ردیف از درخواست sweep (رفت و برگشتی)متناظر است. روش های مختلف در هم آمیختگی حروف SCAN ممکن است ردیف های متفاوت از عکس رمزدار ایجاد کند. با تقلید از روش ایجاد یک ترکیب از حروف SCAN یک رشته ی SCAN تولید می شود. این رشته درخواست sweep عکس اصلی را تعریف می کند. سپس این سیستم عکس اصلی را بررسی می کند. به علاوه رشته های SCAN برای کدگذاری در حوزه ی تجارت به کار می روند. از آن جا که مشتری های غیرقانونی نمی توانند رشته ی SCAN صحیح را بدست آورند، عکس اصلی از دستبرد مصون خواهد بود. در این روش هیچ تصویر بسته ایی وجود ندارد، بنابراین بی فایده است که عکس کدگذاری یا به درستی بازچینی شود.

"کو "یک روش رمزگذاری پیشنهاد داد که مربوط به تحریف عکس است. در این روش تصویر رمزگذاری شده با استفاده ی متناوب از طیف فاز عکس معمولی و عکس کلیدی بدست می آید. چون طیف فاز عکس رمزگذاری شده به

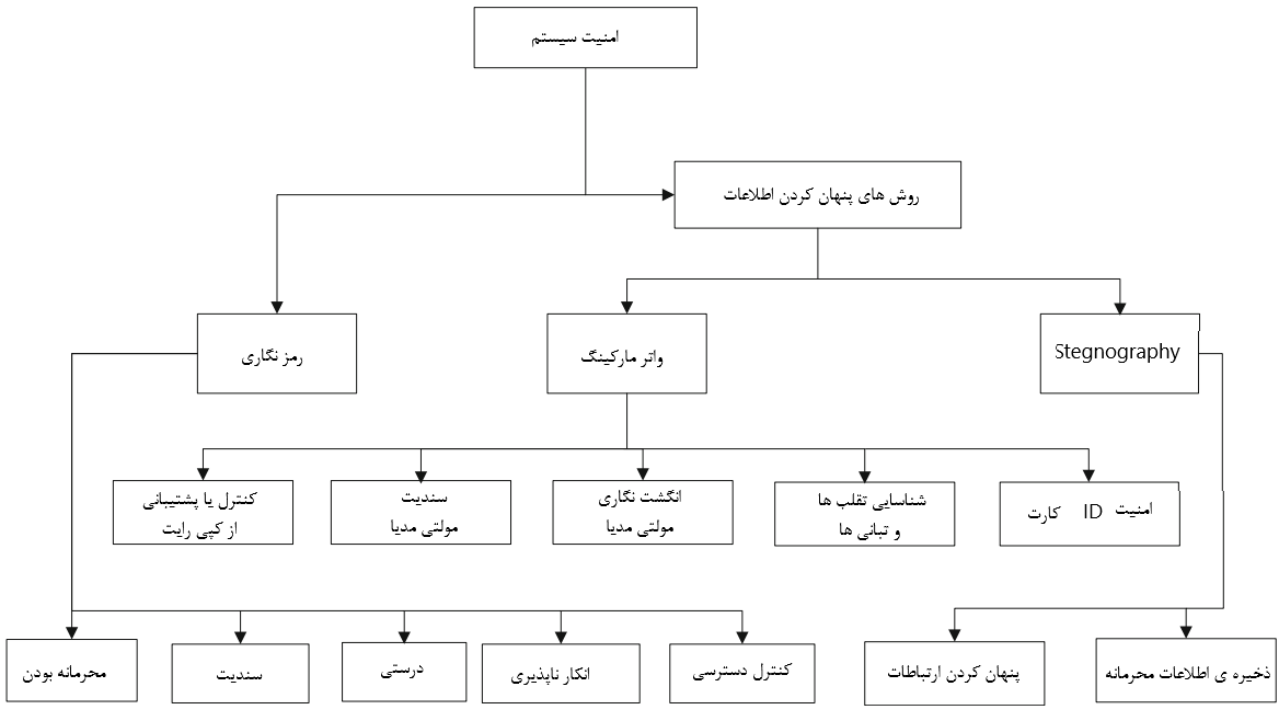
طور تصادفی تغییر می کند، شکل عکس غیرقابل تشخیص است. در طول این خطوط این روش محافظت شده است، اما هیچ تراکم عکسی وجود ندارد (شکل های 1و 2و 3و 4و 5).



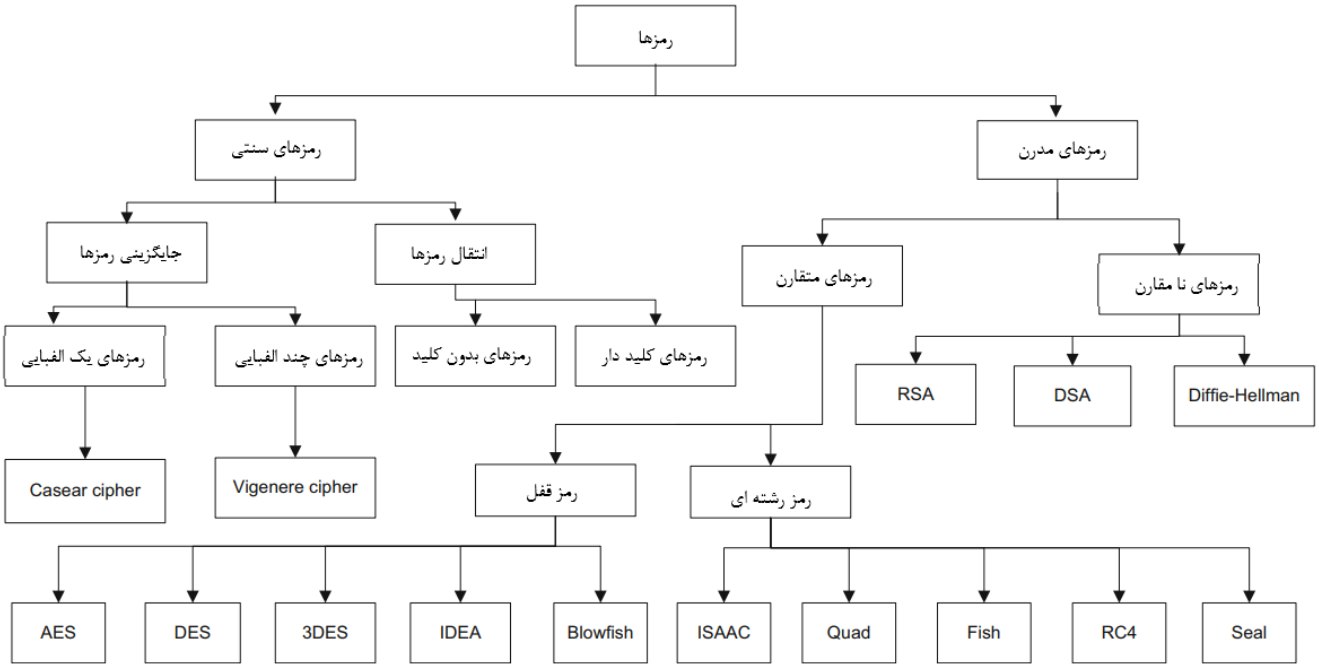
شکل1. دیاگرام بسته ی رمزگذاری و رمز گشایی



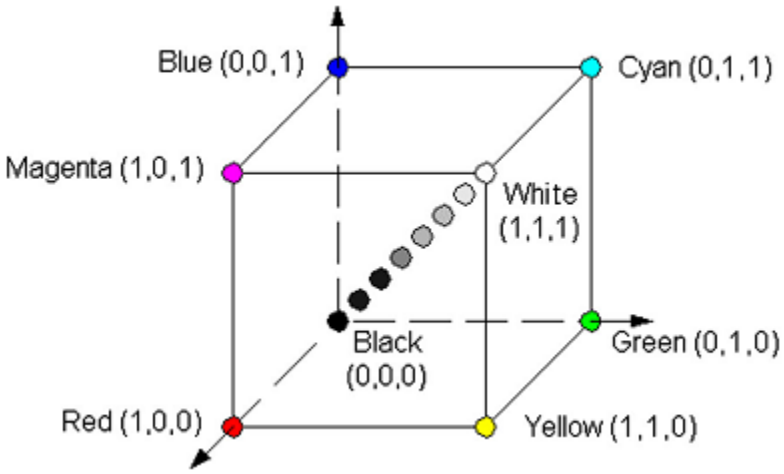
شکل2. ساختار روش رمز گذاری عکس آشوبی



شکل3. دسته بندی روش های امنیت اطلاعات و کاربردهای آن



شکل 4. دسته بندی الگوریتم های رمز نگاری



شکل 5. فضای رنگی RGB

"چانگ و لئو" یک روش رمزگذاری برای دست یابی به تراکم و هدف رمزگذاری به کار بردند. در روش آن ها ساختار داده ی درختی چهارگانه و زبان scan به طور مجزا مورد استفاده قرار می گیرند. در این روش ابتدا عکس اصلی را با استفاده از درخت چهارگانه فشرده می کنند و سپس داده ی فشرده شده را به وسیله ی SCAN رمزگذاری می کنند . در طول این فرآیند عکس به طور هم زمان لایه بندی و بازچینی می شود. درخت چهارگانه به طور کلی مهندسی ایجاد

لایه های متراکم است. ممکن است روش چانگ و لئو به اندازه ی کافی ایمن نباشد تا بتواند با بعضی حملات غیرقانونی مثل حمله ی جدول چیدمانی و حمله ی مجاور و ....مقابله کند. "الکسوپولز و همکارانش" یک روش رمزگذاری برای بازچینی 2D تصاویر سیاه سفید با استفاده از کلاس بزرگتری از فراکتال ها ارائه کردند.

"یانگ و کیم " روشی برای رمزگذاری عکس و مقایسه ی تغییرات جهت بررسی امنیت ارائه دادند. این روش از یک فرآیند هولوگرافیک استفاده می کند که در آن یک عکس کدگذاری شده -به دلیل امپدانس بین دو موج منتقل شده از طریق یک تصویر ID و با ارائه ی یک عکس مرجع به عنوان کلید رمزگذاری -می تواند به صورت 3D مشاهده شود. آن ها نشان دادند که روش پیشنهادیشان عکس کدگذاری شده ی معتبری ایجاد می کند که می تواند مشوق ساخت کارت باشد.

در سال 1996، "اسچرینگر و پیچلر" آیتم دیگری ارائه دادند که به وسیله ی استفاده ی مکرر از عملکردهای جانشینی و استحاله، بخش های بزرگی از محتوای ساده را بازچینی می کند. نقشه ی ارائه شده تغییرات پارامتریک در بخشهای داده را به کار می برد(برای مثال عکس ها) که این تغییرات به وسیله ی چهارچوب های کاری آشفته ی خاص ایجاد می شوند.

"فردریش" یک الگوریتم رمزگذاری نشان داد که می تواند نقشه های دو بعدی بی نظم قابل معکوس معینی ایجاد کند تا طرح های رمزگذاری قفل متقارن جدیدی بسازد. این طرح به طور ویژه برای رمزگذاری اندازه ی داده ی جایگزین مثل عکس های دیجیتال ارزشمند است. در سال 1998، "باپتیتا" پزوهشی مبتنی بر رمزهای قفل آشوبی ارائه داد.

"گو و ین" در رفرنس 22 یک الگوریتم رمزگذاری عکس آینه ایی موثر معرفی کردند. با در نظر گرفتن یک جانشینی دوگانه ی ایجاد شده در یک سیستم آشوبی ، عکس در هر الگوریتم درهم ریخته می شود. این الگوریتم ماهیت چندوجهی محاسباتی پایین و امنیت بالایی ، بدون پیچیدگی دارد.

"ین و گو" یک الگوریتم رمزگذاری/ رمزگشایی عکس و ساختار VLSI آن را ارائه دادند. همان طور که به وسیله ی سکوئنس دوتایی آشوبی نشان داده شد، سطح خاکستری هر سیکل بیتXORED یا بیت XNORED به وسیله ی بیت به یکی از دو کلید مقرر متصل می شود.

در این مقاله "صبحی" از بیان ریاضی Lorenz برای رمزگذاری ، ساخت پایگاه داده های ایمن، فرستادن ایمیل ایمن و انجام FPGA برای عکس های در حال پیشرفت، استفاده کرد. در واقع یک الگوریتم آشوبی برای کدگذاری محتوا و عکس ها به کار گرفته شد. انواع زیادی از رمزنگاری های آشوبی پیشنهاد شده است. ساختارهای آشوبی به دلیل متغیر بودن مدار با توان های Laypunov مثبت و تخصصی، داده را پراکنده می کنند. زمانی که از این ویژگی ها به طور مناسب استفاده شود، رمزنگاری آشوبی باید امنیت بالایی داشته باشد. با وجود این که اکثریت استراتژی های مربوط به امنیت مرسوم از سیستم های آشوبی استفاده می کنند اما به اندازه ی کافی ایمن نیستند. برای مثال پیمان نامه های مربوط به امنیت روی هماهنگ سازی سیستم های آشوبی تمرکز دارد که موجب می شود اطلاعات ارزشمندی به دست مهاجمان بیافتد. رمزنگاری روی کاربردهای فوری نقشه ی آشوبی تمرکز دارد که در مقابل آنالیزهای رمزنگاری

مختلف خطی است. "ماسودا و آی هارا" گونه ی دیگری از سیستم های رمزنگاری آشوبی را پیشنهاد کردند که این مشکلات را تا چند درجه کاهش می دهد. سیستم های رمزنگاری روی نقشه ی tent گسسته تمرکز دارد . به علاوه درصدی از خواص جذاب سیستم رمزنگاری پیشنها شده که کیفیت های دینامیکی را به کار می برد را نشان می دهند. این خواص در رابطه با متن های رمزی نا منظم ممکن است با امنیت زبان رمز به طور نزدیک شناسایی شوند. سیستم های رمزنگاری جدید از یک مرحله برای مربوط ساختن تئوری رایج مورد استفاده در سیستم رمزنگاری و تئوری سیستم دینامیکی استفاده می کنند.

"سینها و سینگ" روش دیگری برای بازچینی عکس جهت انتقال ایمن پیشنهاد دادند.در این روش امضای عکس اصلی به متغیر کدگذاری شده ی مربوط به آن اضافه می شود. کدگذاری عکس با استفاده از کدکنترل خطای مناسب مثل کد BCH انجام شد. در انتها و پس از دریافت و رمزگشایی عکس، علامت محاسبه شده مورد استفاده قرار می گیرد تا اعتبار عکس را تایید کند.

"سالن و همکارانش" یک روش رمزگذاری آشوبی جدید برای عکس براساس نقشه ی "بیکر" پیشنهاد دادند. این الگوریتم که بر پایه ی نقشه ی بیکر است، با استفاده از یک کلید متقارن اصلاح شده می تواند اندازه ی متغیر عکس را پشتیبانی کند وحتما به عکس مربعی برای رمزگذاری نیاز ندارد. بنابراین این الگوریتم شامل توابع مختلف مثل متصل کننده ی پسورد و حرکت دهنده ی پیکسل برای بالا بردن بیشتر امنیت عکس است و دو حالت از عملکردها به ویزه ECB و CBC را پشتیبانی می کند. میزان تکرارهای اجرا شده می تواند به استناد سطح امنیت مورد نیاز برای کاربر تغییر کند. مقاله ی آن ها هم چنین شامل یک نمونه رمزگذاری عکس است. از آنالیزهای انجام شده، نتیجه می شود که سطح امنیت در این روش بالاست چرا که کلیدهایی در این روش ایجاد می شوند که به طور ثابت در الگوریتم مورد استفاده قرار می گیرند.

"شین و همکارانش" روش رمزگذاری عکس چند سطحه را به وسیله ی استفاده از انحصار فاز دوتایی عملکرد OR و روش های تقسیم بندی عکس پیشنهاد دادند. عکس چند سطحه ممکن است به عکس های دوتایی تفکیک شود که سطوح خاکستری یکسان دارند. عکس های دوتایی با استفاده از کدگذاری فاز دوتایی کد گذاری می شوند و پس از

آن به عکس های فاز رندوم دوتایی با استفاده از عملکرد XOR متصل می شوند.در نتیجه تصاویر خاکستری رمزگذاری شده به وسیله ی اتصال هر عکس رمزگذاری شده ی دوتایی حاصل می شود.

در سال 2003" بل خوچ و کیدوای" از یک نقشه ی آشوبی یک بعدی استفاده کردند . در روش آن ها نشان داده شد که می توان از چندین کلید مثل حالت شروع، پارامترهای خروجی و مقدار تکرارها، برای رمزگذاری عکس های دوتایی استفاده کرد. تعیین حساسیت جهت معرفی حالت یک بخش برتر در رمزگذاری آشوبی انجام شد.

"وانگ ینگ" و همکارانش که از رمزگذاری عکس به علت خودتشابهی و خواص روانشناسی واهی عکس ناامید شده بودند، از اولین سیستم انتقال استفاده کردند و سپس یک نقشه ی غیر خطی به کار بردند تا به طور دایره وار مقادیر پیکسل ها را تکرار کند.

"ژانگ و همکارانش" یک ماتریکس T برای بازچینی عکس به کار بردند و قابلیت پیش بینی آن را نشان دادند. ماتریکس T ساده تر است و دوره ی آن دو برابر طول ماتریکس آرنولد می باشد. ممکن است این ماتریکس به سیستم رمزگذاری عکس و الگوریتم های پیش پردازش در پردازش عکس مثل الگوریتم های واترمارکتینگ متصل باشد.

"دنگ و همکارانش" رمزگذاری عکس را به وسیله ی یک سیستم عصبی آشوبی و نقشه ی cat کامل کردند. در مقاله ی آن ها از شبکه ی عصبی برای ساخت روش آشوبی استفاده شد.

"گو و هان" روش های استحاله و جانشینی را با هم به کار بردند تا الگوریتم رمزگذاری عکس قوی ارائه دهندکه در نتیجه ی آن یک عملیات بهبودیافته و نمونه ی متقاطع مصرفی برای توسعه ی خواص پزدو رندوم و اسپاسم گونه (تشنجی) سکوئنس های آشوبی ارائه شد.

"زائو و ژانگ" طرحی با دو سیستم آشوبی با امکان سرّی بودن بالاتر سیستم های چندگانه به کار بردند. یکی از سیستم های آشوبی برای تولید یک سکوئنس آشوبی مورد استفاده قرار می گیرد که در هر نقطه ی سکوئنس آشوبی به وسیله ی تابع آستانه به رشته ی دوتایی منتقل می شود. سیستم آشوبی دیگر برای ساخت ماتریکس استحاله به کار می رود. در ابتدا، مقادیر پیکسل تصویر ساده به طور رندوم و با استفاده از رشته ی دوتایی به عنوان رشته ی کلیدی تنظیم می شود. سپس، عکس تغییر یافته دوباره به وسیله ی ماتریکس استحاله رمزگذاری می گردد.

روش رشته ی رمز در چندین نوشتار مورد استفاده قرار گرفته است، که در ادامه در مورد برخی از آن ها بحث خواهیم کرد. "نیه و همکارانش" یک روش رمزگذاری هیبریدی برای عکس رنگی مبتنی بر سیستم چند آشوبی به کار بردند. آن ها در روش های بازآرایی آشوبی بیت BCR و PCS را در نظر گرفتند. ابتدا یک PCS، با یک روش رمزگذاری سریع که می تواند موقعیت هر پیکسل را به نوسان وادراد ، در سراسر خطوط عکس اصلی توزیع شد و با استفاده از 4 نقشه ی آشوبی henon، lorenz ،chau و rossler متصل شد. سپس ، یک CBR که از سیستم آشوبی استفاده می کند تا اصلاح کدهای آشوبی در سیکل ها را انجام دهد، متصل شد. ترکیب PCR و BCR فضای کلید عکس ها را 10 و 180 برابر افزایش می دهد و در مجموع خطوط تصویر رمزگذاری شده را از بین می برد، توزیع مشخصات ماتریکس های سطح RGB را مبهم می کند و با موفقیت در مقابل حملات هجومی رمزگشایی از عکس محافظت می کند.

"آرهوما و همکارانش" یک نقشه ی آشوبی خطی تکه ایی (PWLCM) برای ساخت یک سیستم رمزنگاری آشوبی پیشرفته ی دیگر پیشنهاد دادند. ویژگی های PWLCM برای طراحی طرح های رمزگذاری بسیار مناسب هستند. این روش عکس رنگی را به سه بردار منتقل می کند، سپس همه ی مقادیر عددی آن ها را به فضای فاز نقشه ی tent منتقل می کند، وقتی در یک نقطه فضای فاز یک نقشه به 256 فاصله ی فرعی وسیع هم اندازه تقسیم می شود. دقت،کارآیی و امنیت طرح رمزگذاری پیشنهاد شده بررسی و قابلیت آن برای رمزگذاری عکس نشان داده شد. فضای کلید 1093 است که اندازه ی فضای کلید بسیار کوچکی است که نشان می دهد مقاومت آن در برابر حملات به دلیل مقادیر بالای NPCR و UACI بدست آمده زیاد است. به علاوه انتروپی در این روش 7/9551 است که نشان می دهد فقط اندازه ی کوچکی از داده ها گم شده اند.

در رفرنس 37، "موشیر و همکارانش" الگوریتم رمزگذاری پیشنهاد دادند که از سه نقشه ی آشوبی گونانوگون بهره می برد. در ابتدا ، آن ها یک عکس را به قفل های 8×8 پیکسلی تقسیم کردند، سپس همه ی قفل ها با استفاده از نقشه ی Cat در هم آمیخته شدند. در مرحله دوم، نقشه ی Cat دوباره به همه ی قفل های توزیع شده متصل شد. در مرحله ی سوم، دوباره یک آمیزه با استفاده از نقشه ی cat ساخته شد تا پیکسل های عکس نهایی به دست آید.

در این نقطه تصویر نهایی با استفاده از نقشه ی منطقی یک بعدی رمزگذاری می شود . نتایج آزمون آن ها نشان داد که این روش فضای کلید غیرقابل قبولی ایجاد می کند که حدود 10112 است و دارای حساسیت بالایی برای تغییرات کم در کلیدهای رمز می باشد. رابطه بین تصویر رمزگذاری شده و تصویر اصلی حدود 0/0095 است که نشان می دهد تصویر رزمگذاری شده سوای تصویر اصلی است. آنتروپی گزارش شده ی تصویر رمزگذاری شده بزرگ است که نشان می دهد فقط اندازه ی کمی از داده ها گم شده اند.

به طریق مشابه "وی و همکارانش" رمزگذاریی عکس را با دیدگاه موجود در رفرنس 37 رمزگذای کردند که تفاوت آن با رفرنس 37 استفاده از سیستم های فوق آشوبی 4D بود. آن ها 4 سکوئنس آشوبی از سیستم های فوق اشوبی 4D تولید کردند. در نقطه ی رمزگذاری در هر کانال رنگ G،R و B تصویر مبتنی بر سکوئنس های سه گانه با حالت زنجیره ایی قفل رمزی بین عبوری کامل شد. آن ها سپس عکس رمزگذاری شده را به وسیله ی کانال های هر سه رنگ در هم آمیختند. بعد از دورهای زیاد رمزگداری ، تصویر رمزی کامل شد. از رفرنس 38 واضح است که ضرایب هم بستگی تصویر رمزگذاری شده به طور چشمگیری کاهش یافته اند و هم چنین نتیجه گرفته شد که تغییر کوچکی در فضای کلید می تواند در یک تصویر بازچینی نشده به طور کامل حاصل شود.

"کمالی و همکارانش" یک طرح رمزگذاری ایجاد کردند که اصلاح استاندارد رمزگذاری پیشرفته (AES) است و روش رمز قفل شناخته شده در رمزگذاری داده است. اصلاح با استفاده از حرکت و انتقال های ردیفی انجام می شود، به این صورت که حتی اگر مقادیر اولین ردیف و ستون وجود داشته باشند، ردیف های اول و بعدی بدون تغییر باقی می مانند، سپس هر بایت در ردیف های دوم و سوم به طور سیکلی به راست حرکت می کند. دوباره ، اگر ردیف های اول و سوم تغییر نکنند، هر بیت از ردبف های دوم و چهارم به سمت چپ حرکت داده می شوند. این روش های اجرای قوی در مقابل حملات آماری را نشان می دهد.

"آی هوانگ و همکارانش" روش انتقال عکس رنگی RGB مبتنی بر نقطه ی منطقی و الگوریتم لغو LSB را پیشنهاد دادند. در ابتدا، نقشه ی منطقی از سه سکوئنس آشوبی و ماتریکس هایG، R و B که به وسیله ی سکوئنس های آشوبی جایگزین شده بودند، استفاده کرد. در دراز مدت الگوریتم های لغو LSB برای قرار دادن عکس رمزگذاری شده

روی عکس حامل از طریق انتقال مورد استفاده قرار می گرفت. این روش امنیت بالا، سرعت عملکرد بالا و کلید رمز پایین برای هر رنگ تصویر دارد و برای انتقال امنیت عکس رنگی به طور گسترده در طول یک سیستم مناسب است.

در رفرنس 41 یک روش رمزگذاری عکس رنگی که از نقشه ی آشوبی منطقی دو مرحله ایی استفاده می کند، پیشنها شده است. برای اولین مرحله ، نقشه ی منطقی مورد استفاده قرار گرفت تا پیکسل های عکس اصلی را جایگزین کند . برای مرحله ی دوم، نقشه ی منطقی در فرآیند انتشار مورد استفاده قرار می گیرد . همان طور که به وسیله ی آنالیزهای اجرایی گزارش شده در رفرنس 41 نشان داد شده است، این روش به سطح بالایی از امنیت نیاز دارد که برای رسیدن به آن سرعت رمزگذاری برای اندازه ی متغیر عکس کاهش می یابد. به طور مستند هم چنین مشاهده شد که کیفیت بالای رمزگذاری با فضای کلید نسبتا کوچکی به دست آمد. به علاوه مشاهده شد که عکس اصلی از عکس رمزگذاری شده مستقل است و در برابر حملات گوناگون به دلیل تخمین هم بستگی حداقل- که 0/0013 بدست آمد- ایمن است.

"مستان" و همکارانش یک روش رمزگذاری عکس رنگی غیر خطی پیشنهاد دادند که ماتریکس انتقال مثل انتشار پیکسل و اجرا را در بر می گیرد . در ابتدا روش انتشار به طور اتوماتیک برای هر کانال از عکس رنگی هم با استفاده از پیکسل منفرد و هم انتشار پیکسل قفل اعمال شد. در نقطه ای بین سه کانال R، G و B بین پیکسل ها اجرا به صورت مستقل انجام می شود. این تکنیک به ویژه برای زمینه های حساس مثل پزشکی که کوچک ترین خطایی یک زندگی را نابود می کند، طراحی شده است و سریع تر از AES است و می تواند به طور پیوسته در انتقال عکس ایمن مورد استفاده قرار گیرد.

در رفرنس 43، " پاریک و همکارانش" الگوریتم رمزگذاری عکس دیگری پیشنهاد دادند که مبتنی بر جایگزینی پیکسل هاست که عکس را به قفل های ترکیبات رنگی تقسیم می کند. سپس هر بخش رنگی در هر قفل به وسیله ی عملکرد XOR تغییر می کند. این الگوریتم ساده، سریع و حساس به کلید رمز است ، زیرا از فضای کلید 2120 استفاده می کند که روش آن ها را در شرایط مرتب کردن/ انتقال عکس های با امنیت بالا مناسب تر می سازد.

یک روش برای رمزگذاری عکس که مبتنی بر حرکت ردیف های و ستون های عکس است به وسیله ی "ابوقارا و همکارانش" پیشنهاد شد. با استفاده از حرکت جدولی که به وسیله ی HASH تولید شده بود، تصویر اصلی به قفل های3×3 پیکسلی تقسیم شد. در یک نقطه قفل ها قبل از این که باز چینی شوند، بیشتر در سراسر ردیف ها و ستون ها حرکت می کنند. در رفرنس 44 مشاهده می کنیم که یک رابطه ی نزدیک بین عکس اصلی و عکس رمزگذاری شده وجود دارد که این نزدیکی به وسیله ی مقدار ضریب های هم بستگی مثل 0/0078- ثابت می شود. این مطلب نشان می دهد که فاصله ی پیکسل های مجاور در یک عکس معمولی از پیکسل های مجاور در عکس رمزگذاری شده کمتر است، که حاکی از انطباق پایین است. از طرف دیگر، به دلیل مقدار آنتروپی بالای به دست آمده ، ممکن است اظهار شود که روش ارائه شده در رفرنس 20 مخالف اصطلاحات مختلف امنیتی است.

روشی در رفرنس 45 استفاده شد که حرکت قفل های عکس و AES را به هم متصل می کند. ابتدا، یک تابع HASH برای ایجاد یک حرکت جدولی جهت حرکت قفل های عکس مورد استفاده قرار می گیرد. سپس، عکس حرکت داده شده به الگوریتم رمزگذاری AES انتقال داده می شود . روش آن ها ظرفیت بالایی برای بازچینی گسترده ی مجموعه های داده به صورت کارآمد و پیش رونده دارد، زیرا مقادیر VPCRوUACI در این روش مقادیر استاندارد بسته ایی هستند که به ترتیب 99/6689 و 27/7599 درصد می باشند. به علاوه مقدار هم بستگی نشان می دهد که عکس اصلی نزدیک ترین مقادیر بین همسایگانش را نسبت به پیکسل های مجاور در عکس رمز گذاری شده دارد که به وسیله ی محیط، سازگاری پایین را ثابت می کند.

به طور قطع یک مسئله ی بحرانی در انتقال عکس های پیشرفته در سیستم های باز مثل اینترنت وجود دارد. رمزگذاری عکس به طور قطع یک راه حل مفید برای حل این بحران است. در بین طرح های رمزگذاری موجود، روش های مبتنی بر در هم ریختگی، عملکرد سریع ، کارآمد و الگوریتم های بسیار ایمنی دارد. یکی از جدیدترین سیستم های رمزگذاری عکس کارآمد مبتنی بر نقشه های ساختاری اجرای انتشار و آشوبی در رفرنس 46 ذکر شده است. از طرف دیگر در رمزگذاری پیام ساده، همان طور که به وسیله ی ایجاد کنندگان روش گزارش شده است، امنیت کامل فراهم می شود، چرا که الگوریتم بیش از دو بار تکرار شده تا ظرفیت بالایی در برابر حملات مختلف ایجاد گردد. هدف این

مقاله، بالا بردن تاثیر پذیری روش آن ها برای پیام ساده است. در نتیجه، تعداد اجراها به طور چشم گیری افزایش یافت تا امنیت کلی سیستم رمزنگاری عکس ایجاد شود. بعد از اثر بررسی های مختلف و بازتولید ماشینی تایید شد که الگوریتم جدید امنیت بالایی دارد و در عمل برای عکس می تواند مورد استفاده قرار گیرد.

در رفرنس 48 یک سیستم رمزنگاری عکس مبتنی بر سیستم موقعیت چند پیکسله و عملکرد برش کوتاه مرحله ایی پیشنهاد شده است. با مقایسه و توصیف روش رمزگذاری عکس رنگی ، نویسندگان روش موقعیت چند پیکسله را به کار بردند تا عکس رنگی فقط در کانال فضایی کدگذاری شود. سپس استراتژی پیشنهاد شده می تواند ویژگی های غیر خطی برای سیستم رمزنگاری و مراتب مختلف فرار از حملات موجود به ویژه حملات تکراری را ایجاد کند. نتایج بازتولید اجرا می شوند تا امنیت و تاثیر اجرای سیستم پیشنهاد شده را نشان دهد.

یک طرح رمزگذاری عکس جدید که روی اجرای ماتریکس سطح بیتی و قفل انتشار تمرکز دارد ، در رفرنس 49 ارائه شده است . در ابتدا، تصویر ساده با استفاده از یک ماتریکس تصادفی به دو قفل 8×8 پیکسلی تقسیم می شود، سپس هر قفل به یک ماتریکس موازی سه بعدی 8×8×8 تبدیل می شود که عمدتا به صورت یک مکعب 6 جهت دارد. اجرا به وسیله ی تکرار ماتریکس سه بعدی و با استفاده از چرخش ماتریکس که بستگی به تصویر اصلی در جهت های مختلف دارد، روی می دهد. به علاوه ، قفل انتشار مورد استفاده قرار می گیرد تا توزیع تغییرات قابل اندازه گیری عکس بعد از در هم ریختگی را بیشتر کند. نتایج بررسی و آنالیزها نشان داد که طرح می تواند امنیت بالایی به دست آورد، به طوری که برای یک حالت موازی مناسب باشد و بتواند در سیستم متناظر برخلاف توان نویز عمل کند.

3.1.2. محدوده ی فرکانس

"سین ها و همکارانش" استراتژی دیگری برای رمزگذاری عکس سیاه سفید با استفاده از انتقال چیدمان سه بعدی پیشنهاد دادند. برای شروع، عکس به صفحات بیتی منتقل می شود که هر صفحه ی بیتی به قفل های کوچک بیشتری تفکیک

می گردد. انتقال چیدمان سه بعدی هر قفل را منتقل می کند و با این انتقال سطح در سه بعد، تغییر می کند. آن ها

دو انتقال فوریه ی کسری (FRFT) به کار بردند، اولین انتقال FRFT برای کدگذاری عکس مورد استفاده قرار می گیرد و سپس یک عملکرد با کد مرحله ایی رندوم بازتولید می شود. در حالی که دومین انتقال FRFT برای به دست آوردن عکس رمزگذاری شده مورد استفاده قرار می گیرد و با استفاده از FRFT و مدهای مرحله ی رندوم، امنیت روش به دست می آید.

در رفرنس 51 روش رمزگذاری شامل سه بیان است که چرخش فضای رنگی نامیده می شود. فضای رنگی مربوط به عکس رنگی اصلی در ابتدا به طور کامل عکس رنگی از فضای RGB را به فضای مکمل RGB تبدیل می کند. سپس هر بخش رنگی جداگانه انتقال داده خواهد شد. کسر Merllin آن ها را نگه داری کرده و بسته به هدف رمز گذاری هر بخش را منتقل می کند. در نهایت جهت دست آوردن امنیت بالا ، بازچینی پیکسل ها در سه بعد انجام خواهد شد. استدلال ما این است که فضای کلید بزرگ دراستراتژی آن ها می تواند یک رمزگذاری حساس به خطر ایجاد کند.

"ابوتراب " یک سیستم پیشنهاد داد که عکس های رنگی ایمن در نور با استفاده از انتقال آرنولد در محدوده ی انتقال چرخنده به دست می آیند. در استراتژی آن ها، عکس رنگی به بخش های منفرد G،R و B تقسیم شد و سپس هر بخش به طور مستقل با استفاده از اعمال ماسک فاز تصادفی اول رمزگذاری شد و سپس اولین دستور انتقال آرنولد اجرا شده و نهایتا ، انتقال چرخنده صورت گرفت. ماسک فاز تصادفی دوم روی نقشه ی منتقل شده ی چرخنده قرار داده شد و اطلاعات بیشتر با استفاده از دستور دوم انتقال آرنولد و انتقال چرخنده اجرا شد. در واقع در این روش از دو انتقال استفاده می شود: انتقال آرنولد و انتقال چرخنده که هر دو در رفرنس 52 به کار گرفته شده اند و به عنوان کلیدهای اضافی برای رمزگذاری بدون بارچینی مورد استفاده قرار می گیرند که ممکن است به طور مشابه مقاومت در برابر حملات و امنیت را بالا ببرد.

در رفرنس 53 ، یک کانال منفرد سیستم رمزگذاری عکس رنگی پیشنها شده است. این استراتژی با استفاده از شبکه ی کامپوزیت ارتوگونال و کدگذاری فاز تصادفی دوگانه ساخته شده است. در این روش ابتدا یک تصویر رنگی به بخش های R، G و B تقسیم شده و بر شبکه ی کامپوزیت ارتوگونال تطبیق داده خواهد شد. سپس شبکه ی کامپوزیتی پیچیده به وسیله ی روش رمزگذاری فاز تصادفی دوگانه مرتب رمزگذاری می شود. این روش نشان داد که ترکیب کد

گذاری فاز تصادفی دوگانه و شبکه ی کامپوزیت ارتوگونال ماهیت طبیعت چندوجهی برای سیستم رمزگذاری فراهم می کند و هزینه ی رمزگذاری را کاهش می دهد.

در رفرنس 54 یک الگوریتم رمزگذاری عکس رنگی که از انتقال پیوسته در محدوده ی انتقال چرخنده استفاده می کند، پیشنهاد شده است. در ابتدا انتقال پیوسته به بخش های RGB عکس رنگی متصل شده و روی بخش های واقعی و تصوری و بخش تکراری عکس متمرکز می شود. سپس، کیفیت های پیکسل عکسR ، G و B به وسیله ی بازچینی با روش زاویه ی تصادفی تغییر می کند و عکس حاصل با استفاده از انتقال چرخنده منتقل شده و دوباره به وسیله ی انتقال پیوسته ی دوم در هم آمیخته می شود. نتایج نشان داد که الگوریتم پیشنهادی آن ها امنیت بالایی دارد.

یک کانال رمزگذری عکس رنگی منفرد پیشنهاد شده است که روی انتقال فوریه ی کسری تکراری و نقشه ی منطقی دو زوجی متمرکز است. در ابتدا، یک عکس سیاه سفید با سه کانال عکس رنگی تشکیل می شود و با استفاده از توالی مجموعه های آشوبی که به وسیله ی نقشه ی منطقی دو زوجی ایجاد شده است، جایگزین می شود. در نهایت ، جایگزینی عکس با جایگزینی به وسیله ی سه بخش به جای یک بخش کاهش می یابد. بنابراین دو بخش اول با انتقال فوریه ی کسری تکراری متمرکز منفرد کدگذاری می شود و بخش سوم به صورت متن رمزی سیاه سفید نهایی با توزیع نویز ثابت سفید کدگذاری می شود که در بعضی درجه ها خاصیت استتاری دارد. در رمزگذاری و تجسم حاضر، جایگزینی آشوبی یک عکس سری غیر خطی و بی نظم هم درمحدوده ی فضایی هم در محدوده ی فرکانس می سازد. در این روش استفاده از الگوریتم انتقال فوریه ی کسری تکراری پیشنهاد شد که سریع تر است. بنابرای نقشه ی رمزگذاری، فضای کلید سیستم رمزنگاری را تقویت می کند. نتایج شبیه سازی و بررسی ها امنیت قابل دست یابی و کارایی این سیستم را تایید می کند.

در بعضی اپلیکیشن های خاص ، فقط بخش هایی با داده ی معنادار در نظر گرفته می شود تا امنیت بهتری ایجاد کنند در حالی که بخش های دیگر می توانند از رمزگذاری رها باشند.این در حالی است که ، اکثر طرح های امنیت محیط فعلی به جای داده ی معنا دار فقط شامل بیت ها و پیکسل ها برای رمزگذاری است. با وجود چنین مسئله ایی، نویسندگان یک طرح رمزگذاری عکس کم وزن مبتنی بر لبه پیشنهاد دادند که از انتقال لغو شده ی برگشت پذیر

آشوبی و انتقال کسینوس کسر گسسته استفاده می کند. یک عکس ابتدا به وسیله ی تشخیص لبه ی متمرکز در ساختار CNN توسعه یافته و در محدوده های متفاوت قرار می گیرد تا اطلاعات زیادی در عکس بررسی شود . نتیجه، یک عکس دوگانه است که در "1" پیکسل ها شناسایی شده و تصویر اصلی به قفل های پیکسل بدون پوشش با یک روش به طور جداگانه تقسیم می شوند، خواه یک قفل بازچینی شده باشد یا به وسیله ی مقایسه ی قفل های بررسی شده فهمیده شود که قفل، معنادار است. قفل معنادار به وسیله ی انتقال مخفی برگشت پذیر و پس از آن به وسیله ی پارامترهای انتقال کسینوس کسر گسسته گروه های مختلف اجرا می شود و این دو انتقال به وسیله ی نقشه آشوبی دو بعدی کنترل می گردند. نتایج آنالیزها تشکیل ترفندهای مهم یک عکس که عمدتا به وسیله ی کدگذاری نیمی از پیکسل ها در نمایش نرمال مخفی می شود را نشان داد. کلیدها حساسیت بالایی دارند و تا میزان زیادی می توانند با حملات مقابله کنند.

یک طرح جدید برای لغو داده ی نوری (رمزگذاری) مربوط به عکس های دو بعدی به وسیله ی انتقال عکس با روش های بازچینی در فضاهای فوریه ی کسری در رفرنس 57 پیشنها شده است. در ابتدا عکس به طور تصادفی با استفاده از الگوریتم انتقال چیدمان حرکت کرده و سپس با روش انتقال آرنولد بازچینی می شود. عکس مخلوط شده سپس در محدوده ی فوریه کسری به طور تصادفی کدگذاری می شود. سپس این روش ها مکررا انجام می شوند. پارامترهای طراحی ساختار الگوریتم که عبارت اند از : لیست های جایگزین چیدمان ، فرکانس های آرنولد و گروه های فوریه ی کسری، ساختار فضای بزرگ کلید و سطح امنیت چهارچوب رمزگذاری پیشنهاد شده را بهبود می دهند. اجراهای نوری پیرامون الگوریتم های اجرای عددی بحث می کنند. نتایج شبیه سازی های عددی در این روش ارائه شد تا قدرت و انعطاف پذیری چهارچوب کاری را نشان دهد.

برای افزایش امنیت روش کدگذاری فاز تصادفی دوگانه ، یک ردیف از دامنه ی طرح، بازچینی شده و درون فرآیندهای رمزگذاری عکس اورده شد. اطلاعات تصادفی حاصل از ماسک فاز دوم در روش کدگذاری فاز دوگانه هم برای مناسب سازی کارآیی بازچینی مورد استفاده قرار گرفت تا فضای ظرفیت و انتقال داده ی کلیدی را تفکیک کند. نحوه ی

عملکرد بازچینی برای تولید کلید قابل پیش بینی نیست. ضمن این که بعضی تولیدات مجدد عددی اصلاح شدند تا درستی طرح رمزگذاری عکس حاصل شود.

یک الگوریتم رمزگذاری جدید عکس دوگانه با استفاده از سیستم بازچینی پیکسل مجاور مبتنی بر آشوب و انتقال چرخنده پیشنها شد. در ابتدا دو عکس به طور جداگانه به عنوان دامنه و فاز مربوط به ظرفیت پیچیده در نظر گرفته شدند . انتقال آرنولد برای بازچینی پیکسل های مجاور ظرفیت پیچیده به کار رفت و انتقال مجدد آرنولد به وسیله ی نقشه ی استاندارد و نقشه ی منطقی به طور مجزا انجام شد . در یک نقطه به وسیله ی انتقال چرخنده، ظرفیت پیچیده تغییر کرد. این دو عملکرد خاص مکررا اجرا شد. پارامترهای چهارچوب در بازچینی پیکسل های مجاور و انتقال چرخنده به عنوان کلیدهای این الگوریتم رمزگذاری ارائه شد. تکرار عددی اجرا شد تا درستی و امنیت الگوریتم رمزگذاری پیشنهادی را آزمایش کند.

یک کانال منفرد رمزگذاری عکس رنگی پیشنهادی روی الگوریتم بارزیابی فاز و نقشه ی منطقی دو زوجی متمرکز شد. در ابتدا، یک تصویر خاکستری با سه کانال از عکس رنگی ساخته شد و سپس به وسیله ی بازآرایی مربوط به مجموعه های آشوبی به وسیله ی نقشه ی منطقی دو زوجی جایگزین شد. هم چنین، عکس جایگزین شده به سه بخش جدید تفکیک شد که هر بخش فقط به یک ظرفیت فاز در فضای فوریه ی کسری با الگوریتم بازیابی فاز کدگذاری می شود. نهایتا، یک عکس به وسیله ی نقشه ی ظرفیت های فازی تشکیل شده و به متن رمزی سیاه سفید نهایی با نویز پشت زمینه ی ثابت تبدیل می شود و به وسیله ی انتشار آشوبی بازچینی می گردد که در بعضی درجات خاصیت استتاری دارد. در زمان رمزگذاری و بدون بازچینی ، با استفاده از جایگزینی آشوبی و انتشار و الگوریتم های تکراری فازی که سرعت اتصال بالایی دارند، مجددا یک عکس ساخته می شود. به علاوه ، طرح رمزگذاری فضای کلید سیستم رمزنگاری را تقویت می کند . نتایج آزمایش و آزمایش امنیت عملی بودن و کاربردی بودن این تکنیک را بررسی کرد.

رمزگذاری عکس و کدگذاری برای امنیت عکس ها در برابر انواع حملات مهم است. در رفرنس 61، روش اول برای رمزگذاری عکس RGB بدون بازچینی از دو مرحله ی ماتریکس تصادفی استفاده شد تا شکل با انتقال موجی گسسته منتقل شده ارائه شود. پس از نقشه های پیشنهادی برای کدگذاری عکس ها فقط درباره ی کلیدها صحبت شده بود

که در روش پیشنهادی ما هم، کلیدها و طرح بازی پارامترهای RMAC مهم هستند. نویسندگان هم چنین در تلاشند تا در صورت امکان کلیدهایی برای بازچینی و کدگشایی عکس RGB ایجاد کنند. شبیه سازی های کامپیوتری با نمونه ی استاندارد و نتایج آن فراهم شد تا توانایی روش پیشنهادی را بررسی کنند. برای تشخیص توان روش پیشنهادی ما و روش های دیگران یک سری آزمایش امنیت انجام دادیم. نتایج نشان داد که این روش می تواند برای انتقال اطلاعات عکس به صوت کارآمد و ایمن مورد استفاده قرار گیرد.

یک روش رمزگذاری عکس دوگانه با استفاده از مزیت پیکسل فاز و کدگذاری فاز در فضای چرخنده پیشنها د شده است. دو عکس به طور جداگانه به عنوان یک عکس مناسب و ظرفیت فاز در الگوریتم رمزگذاری در نظر گرفته شدند. پیکسل های هر دو عکس به طور تصادفی با کنترل ماتریکس مبادله شدند. یک ماتریکس تصادفی به عنوان بخشی از مزیت پیکسل و کدگذاری فاز برای فضای کم در اپلیکیشن انتقال و ذخیره ی کلید مورد استفاده قرار گرفت. برخی نتایج اجرای مجدد عددی برای نمایش اجرا و امنیت رمزگذاری عکس دوگانه حاصل شدند.

یک طرح رمزگذاری عکس چندگانه مبتنی بر انتقال موجی نوری (OWT) و انتقال فوریه ی کسری چند کاناله (Mfrft) در رفرنس 63 پیشنهاد شده است. طرح می تواند با استفاده از مشخصات مربوط به انتقال موجی (WT) و کنترل

چندکاناله ی Mfrft ایجاد شود و خواص ویزه ایی از رمزگذاری عکس چندگانه و عکس منفرد به دست آید. در یک نقطه وقتی رمزگذاری پایان یافت، هر عکس کسر مورد نظر و کلیدهای خودکار را دریافت می کند. در پایان آزمایشاتی جهت بررسی اثر بازچینی انجام می شود. به علاوه تاثیر نوع wt و گروه آزمایش هم بررسی گردید شد و بررسی Mfrft به گونه ایی تخصصی انجام شد. اجرای مجدد عددی، عملی بودن طرح را تایید کرد و انعطاف و توسعه ی طرح را نشان داد، ضمن آن که که مشکل محدوده ی ناکافی تا حدودی برطرف شد. یک وسیله ی در هم آمیختن اپتو الکترونیک حرکت به جلو برای فهم این طرح در رفرنس 63 پیشنهاد شده است.

در رفرنس 65، انتقال فوریه ی کسری چند پارامتر با گروه انتقالش تبدیل به یک بردار واقعی شدند و یک طرح رمزگذاری عکس با امنیت بالا حاصل شده است. این انتقال فوریه ی جدید کسری ، محدودیت اندازه گیری گروه انتقال

را از بین برده و به میزان زیادی امنیت طرح و رمزگذاری عکس پیشنهاد شده در این مقاله را بدون توسعه ی کیفیت چند وجهی و ارزش متناسب توسعه می دهد. نتایج عددی، کارآیی و امنیت این روش رمزگذاری عکس را بررسی می کند. بردار توان انتقال فوریه ی کسری چند پارامتره جمع انواع انتقال فوریه ی کسری سنتی است که انتقال فوریه ی کسری سنتی تاثیر زیادی در کنترل داده و امنیت داده دارد.

یک روش جدید مبتنی بر امپدانس برای رمزگذاری عکس چندگانه به وسیله ی ماسک فاز چند پیکسله (POM) طراحی شده است. داده ی عکس چندگانه می تواند در POM مثل متن رمزی بازچینی شود. بدون انجام هر روش تکراری برای کدگشایی صحیح ، باید متن های رمزی و کلیدهای خصوصی در دسترس باشد. POM های حاصل به صورت تشخیصی هستند. هم چنین مشکل مسئله می تواند به همین ترتیب به طور کامل در میان این POM ها برطرف شود.عکس های بازیابی شده به وسیله ی این روش کاملا رها از نویز حملات متقابل است که موانع گذشته ی مبتنی بر استراتژی های رمزگذاری عکس چندگانه را تفسیر می کند. نتایج عددی برای بررسی درست بودن روش پیشنهادی ارائه شد.

طرح رمزگذاری عکس دوگانه با روش بازچینی پیکسل های نزدیک به هم و انتقال چرخنده ، پیشنهاد شده است. همه ی نویسندگان، تاثیر حملات متقابل جدی وقتی اطلاعات کدگذاری شده تحت نویز یا حمله قرار می گیرد را در عکس های مبتنی بر فاز بررسی کردند. این حملات باعث زوال در تصویر مبتنی بر فاز بازیابی شده خواهد شد و ابهامات دیداری را برای دریافت کننده ی پیام ایجاد می کند و در نتیجه قابلیت عملکرد سیستم رمزنگاری را کاهش می دهد. در این مقاله، در ابتدا تجزیه ی نقطه به نقطه ی در ساختار اصلی انجام شده و سپس یک تغییر مقایسه ایی در طول این خطوط ارائه خواهد شد. نتایج بازتولید های عددی نشان داد که این طرح به خوبی تاثیرحملات را شناسایی می کند و امنیت سیستم رمزنگاری اولی را بیشتر توسعه می دهد.

3.1.3. محدوده ی هیبریدی

در رفرنس 67 یک استراتژی رمزنگاری که با استفاده از انتقال موجی و نقشه ی آشوبی ساخته شده، پیشنهاد شده است. عکس با استفاده از انتقال موجی منتقل می شود تا این که همه ی اطلاعات بحرانی نقشه به پایین فرکانس زیر باند برسد. در طول این خطوط ، یک روش رمزگذاری آشوبی با کیفیت بالا به کار می رود تا ضرایب موجی فرکانس پایین را بازچینی کند، در حالی که XOR در نواحی عکس در پهنای فرکانس بالا عمل می کند. باز تولید موج گونه ی بیشتر، توزیع اطلاعات رمزگذاری شده از پهنای فرکانس پایین به سراسر عکس را در بر می گیرد. بعد از بازچینی آرنولد از تصویر بازتولید شده موجی حاصل ، تصویر منتشر شده تا سطوح رمزگذاری هموار شود. زمان رمزگذاری گزارش شده در این استراتژی 0/266 ثانیه و فضای کلید 2128 است.

" ال لطیف" و همکارانش ترکیبی از فهرست انتقال فیدبک خطی و سیستم های آشوبی در محدوده ی هیبریدی را نشان دادند. در ابتدا عملیات در موقعیت های پیکسل عکس ورودی مبتنی بر نقشه ی آشوبی دو بعدی و در محدوده ی فرکانس اجرا شد. سپس، تصویر حاصل به وسیله ی اعمال عملکردهای اولیه سیستم رمزنگاری ترکیب با LFSR و نقشه ی آشوبی منتشر شد. در اصول نتیجه ی گزارش شده در رفرنس 53، می توان گفت روش آن ها محفوظ از حملات قوی است. هم چنین مشاهده شد که فضای کلید بزرگی برابر 2256 فراهم شده است. آن ها هم چنین زمان رمزگذاری را 0/023 ثانیه ثبت کردند که نشان می دهد روش آن ها بسیار سریع و مناسب برای کاربردهای فوری است. با مقدار آنتروپی 7/999 می توان گفت روش آن ها در برابر هر حمله ای ایمن بوده و امکان حملات حداقل است.

روش های موجود برای رمزگذاری عکس های مبتنی بر تشخیص فشرده معمولا با همه ی ماتریکس اندازه گیری به عنوان کلید سر و کار دارد که کلید بزرگی برای توزیع و ذخیره ارائه می دهد. برای حل این مشکل، الگوریتم جدید هیبریدی رمزگذاری متراکم عکس پیشنها شده است تا تراکم و شبیه سازی رمزنگاری درک شود، که کلید در آن به راحتی توزیع شده یا ذخیره می شود. عکس ورودی به چهار قفل تقسیم شده تا رمزگذاری شود، سپس پیکسل های دو قفل مجاور به طور تصادفی به وسیله ی ماتریکس های تصادفی مبادله می شوند. ماتریکس های اندازه گیری در

تشخیص تراکم با استفاده از ماتریکس های چرخشی و کنترل بردارهای ردیف اصلی ماتریکس چرخشی با استفاده از نقشه ی منطقی انجام می شود. ماتریکس های تصادفی مورد استفاده در مبادله ی پیکسل های تصادفی با ماتریکس های اندازه گیری تعیین می شوند. نتایج شبیه سازی موثر بودن، امنیت الگوریتم پیشنهادی و کارآیی الگوریتم فشرده ی قابل قبول را تایید می کند.

تکنولوژی تشخیص Remote نقش مهمی در زمینه های نظامی و صنعتی بازی می کند . عکس تشخیص Remote ابزار مهمی در زمینه ی اطلاعات به دست آمده از ماهواره هاست که معمولا شامل برخی اطلاعات محرمانه است. برای انتقال ایمن و ذخیره ی عکس های تشخیص Remote ما یک الگوریتم جدید رمزگذاری عکس در قلمرو هیبریدی ارائه دادیم. این الگوریتم از همه ی مزایای رمزگذاری عکس هم در محدوده ی فضایی هم در محدوده ی انتقال بهره می برد. ابتدا، ضرایب ضعیف زیر باند حاصل از تجزیه ی عکس DWT(انتقال موجی گسسته) به وسیله ی سیستم PWLCM در محدوده ی انتقال مرتب می شوند.در مرحله ی دوم ، عکس بعد از IDWT (انتقال موجی گسسته ی معکوس) با نقشه ی منطقی دو بعدی و عملکرد XOR بازسازی شده و در محدوده ی فضایی منتشر می شود. نتایج ازمایشات و آنالیزهای الگوریتم نشان می دهد که این الگوریتم جدید فضای کلید بزرگی در اختیار دارد و می تواند در برابر حملات مختلف مقاومت کند. در ضمن، الگوریتم پیشنهاد شده در عمل بازده رمزگذاری مطلوبی برای نیازهای مورد نظر دارد.

امنیت داده بسیار مهم است، به ویژه در مورد عکس های دیجیتال که با روش های نامناسب رمزگذاری شده اند. بنابراین باید روش جدیدی ارائه شود تا امنیت داده ی عکس حفظ شود. بازچینی عکس یکی از این روش ها است که مقدار پیکسل را تغییر نمی دهد و فقط موقعیت آن را تغییر می دهد تا آن را در برابر حملات ایمن کند. در این مقاله، ما از روش بازچینی عکس در چهارچوب کاری خودمان استفاده کردیم، که باعث رمزگذاری عکس های دیجیتال شد تا آن ها را ایمن تر سازد. در ابتدا انتقال های غیر سینوسی مورد استفاده قرار گرفت، ما اینجا همه ی ترکیبات انتقال های هیبریدی را با استفاده از انتقال Kekre به عنوان پایه ی انتقال با انتقال های غیر سینوسی دیگر کشف کردیم. در مقایسه با انتقال های غیر سینوسی، نتایج ازمایشگاهی خوبی فراهم شد.

امنیت عکس این روزها به دلیل افزایش پیشرفت رسانه ها و توان حملات یک مسئله ی جدی است. در این مقاله بهترین مدل هیبریدی برای رمزگذاری عکس ساخته شده از الگوریتم ژنتیک و تابع آشوبی را معرفی می کنیم. در اولین مرحله از روش پیشنهادی تعدادی از عکس های رمزگذاری شده با استفاده از کلید رمز و تابع آشوبی ساخته می شوند. در مرحله بعدی ، این عکس های رمزگذاری شده به عنوان داده های اولیه برای الگوریتم ژنتیک مورد استفاده قرار می گیرند . در این روش پیشنهاد شده الگوریتم ژنتیک مورد استفاده قرار می گیرد تا نتیجه ی بهینه ایی فراهم کند و در آخرین مرحله بهترین عکس رمزی براساس محاسبات ضریب هم بستگی و آنتروپی انتخاب می شود. عکسی با پایین ترین ضریب هم بستگی و بالاترین آنتروپی به عنوان بهترین عکس رمزی انتخاب می شود. در این مقاله ابتدا الگوریتم ژنتیک را برای رمزگذاری عکس ها به کار می بریم . آنتروپی و ضریب هم بستگی فراهم شده به وسیله ی این روش به ترتیب 7/9978 و 0/0009- هستند.

" کریشنا مورتی و مورلی" یک تکنیک رمزگذاری جدید ممکن در محدوده ی هیبریدی پیشنهاد دادند که روش چندگانه ی تحلیل الحاقی رمزگذاری در محدوده ی فرکانس با انتقال کسینوسی گسسته (DCT) و محدوده ی فضایی برای در هم آمیختن پیکسل ها را به کار می برد . ابتدا، عکس اصلی به قفل های معنادار و بی معنا با استفاده از اپراتور شناسایی لبه ی Prewitt تقسیم می شوند و قفل های با معنی به وسیله ی نقشه ی آرنولد در هم آمیخته شده، سپس DCT معکوس اعمال می شود و پیکسل ها در قفل ها با خروجی گسسته از نقشه ی منطقیXOR می شوند. در نهایت، فرآیند انتشار اعمال می شود تا عکس رمزگذری شده ی نهایی حاصل شود و شبیه سازی های عددی امنیت و قدرت طرح رمزگذری پیشنهادی را نشان دهد.

همه ی سیستم های رمزگذاری عکس در محدوده ی منفرد هستند . سیستم محدوده ی هیبریدی (محدوده ی فرکانس و زمان) پیشنهاد شده است تا یک سیستم را امن تر سازد. ما از نقشه های آشوبی برای تولید عکس پزدو رندوم استفاده می کنیم. چون نقشه های آشوبی ویژگی های خیلی خوبی دارند ، به ما کمک خواهد کرد تا عکس را با روش امن تری رمزگذاری کنیم. در سیستم پیشنهادی ما، دو واحد را به کار می گیریم : واحد انتقال و واحد

جایگزینی. انتقال فوریه ی گسسته و انتقال موجی گسسته را برای عکس اجرا می کنیم. واحد انتقال از نقشه ی tent استفاده می کند و واحد جایگزینی نقشه ی برنولی را به کار می برد.

3.2. رمزگذاری انتخابی

در عکس معمولی و طرح های بیمه ی محتوای ویدیو کل مفهوم رمزگذاری می شود. رمزگذاری انتخابی یک استراتژی است که فقط بخشی از رشته ی بیتی فشرده شده را کدگذاری می کند و فقط شامل رمزگذاری یک زیر مجموعه از داده هاست. بنابراین رمزگذاری انتخابی، رمزگذاری جزئی هم نامیده می شود. یک ویژگی ضروری رمزگذاری انتخابی این است که رشته ی بیتی رمزگذاری شده می تواند با استفاده از کدبـَردارهای استاندارد کدبرداری شود . بنابراین هم بیت های رمزگذاری شده و هم بیت های رمزگذاری نشده از رشته ی بیتی لایه ایی ممکن است صراحتا کدبرداری شده و نشان داده شوند. بنابراین رمزگذری انتخابی مربوط به رمزگذاری سازگار با موقعیت است. با ظرفیت رمزگذاری انتخابی ، پیشنهادات زیادی می توانند اجرا شوند. سیستم رمزگذاری انتخابی شبیه به استراتژی رمزگذاری کامل نیست و فقط مناطق با ارزش در عکس داده شده را کد گذاری می کند. نکته ی مهم استراتژی رمز گذری انتخابی این است که می تواند بدون بررسی، امنیت و ضروریات محاسباتی مورد نیاز را ایجاد کند. کاربرد روش رمزگذاری انتخابی در اپلیکیشن های پیشرفته ی اساسی است که به طور فزاینده در اندازه گیری داده بزرگ مورد استفاده قرار می گیرند. تحقیق و توسعه ی این روش باید تا آن جا ادامه یابد که ضروریات محاسباتی برای امنیت محیط در هم آمیخته را حداقل کند. به دلیل مسئله ی پیچیدگی محاسبات، در رمزگذاری جزیی نگرانی هایی وجود دارد.

روش های رمزگذاری عکس جزئی روی تشخیص و مجزا کردن اطلاعات به دو دسته داده ی حساس و غیر حساس متمرکز است. دراینجا مقایسه ایی ارائه می دهیم که به شرایط مرکزی طرح رمزگذاری جزئی بستگی دارد، که بخش رمزگذاری شده نباید مستقل از سطوح رمزگذاری شده باشد. بنابراین طرح پیشنهادی که در این مقاله بررسی خواهیم کرد با فرض این که این طرح در محدوده ی شرایط رمزگذاری جزئی است، بررسی می شود.

در این قسمت، طرح رمزگذاری جزئی با استفاده از تلاش های تحقیقاتی زیادی توصیف شده است که در این دسته بندی همه ی محدوده ها به ویزه فضایی، فرکانس و هیبریدی لحاظ شده است. در قسمت بعدی روی روش های موجود در مقالات با فرض محدوده های ذخیره و روش های رمزگذاری، مثل روش های رمز قفل و رمز رشته ایی تمرکز خواهیم کرد.

3.2.1. محدوده ی فضایی

در سال 2002 ، "ون دروگن بروک و بندت" روش های رمزگذاری انتخابی برای تصاویر غیر فشرده (شبکه ایی) و عکس های فشرده (JPEG) پیشنهاد دادند. طبق مدل ون دروگن بروک و بندت حداقل 5-4 صفحه ی بیتی مهم باید رمزگذاری شود تا زوال دیداری در عکس پدید آید.

"پرودسر، اسچمید و یوهی" یک الگوریتم رمزگذاری انتخابی برای تصاویر غیر فشرده پیشنهاد دادند که معکوس سیستم ون دروگن بروک و بندت است. در عکس شبکه ایی که شامل صفحات 8 بیتی است، الگوریتم اسچمید و یوهی فقط صفحات بیتی معنا دار را کذ گداری می کند . سیستم رمزنگاری اصلی پیشنهاد شده برای این تکنیک AES بود. اما ، بدون از دست دادن کلیت ، هر سیتم رمزنگاری سنتی سریع ممکن است جایگزین آن شود.

"رائو" و همکارانش در ابتدا یک عکس را به وسیله ی جداسازی آن به چهار صفحه ی اولیه MSBو چهار صفحه ی نهایی LSB به دو نوع داده ی متصل و نامربوط تقسیم کردند. سپس یک جانشینی پزدو رندوم در داده ی نامربوط به کار رفت تا داده های مشابه را بازچینی کند و در ضمن داده ی نامربوط بدون رمز گذاری باقی بماند ، پس از آن داده ی متصل با داده ی نامربوط با استفاده از رمز، ترکیب شده تا عکس نهایی ایجاد شود. دیده شده است که عکس رمزگذاری شده کیفیت قابل شناسایی ناحیه ی رمزگذاری شده را افزایش می دهد، در نتیجه خطر نیز افزایش می یابد. در طول این فرآیند به مسئله قابل پیش بینی نبودن محاسبات توجه نمی شود.

در رفرنس 80 " وانگ و بی شاپ" مهندسی ساختار کلی رمزگذاری عکس ROI چند سطحه را برای داده ی بیومتریک ارائه دادند. در کار آن ها ، رمزگذاری ROI چند سطحه و RC4 برای کدگذاری یک عکس شبکه ایی غیر فشرده مورد

استفاده قرار گرفت. تفکر پشت روش آن ها این است که برای هر بیننده، فقط بخش های شناسایی شده قابل دیدن است. در واقع ، فرد آزمایش کننده می تواند ماهیت عکس رمزگذاری شده را ببیند که این مطلب اصولی سیستم بیومتریک است. در مرحله ی اول، ROI های مختلف برای هر عکس انتخاب خواهد شد ، که سپس در سه سطح از توان با استفاده از RC4 و الگوریتم انطباق انگشت نگاری رمزگذاری می شود. دیدیم که روش آن ها امنیت اطلاعات عکس بالایی دارد ،اما اندازه فضای کلید (2128) قابل تو.جه است، که نشان می دهد سیستم می تواند به تغییر کوچکی در کلید رمز حساس شود.

در رفرنس 81 استاندارد رمزگذاری پیشرفته ی AES-Rijndael با دقت روی 5 معیار محافظت از داده ی ساده، اندازه ی قفل ها، دور قابل انتخاب، بالا بردن اجرای برنامه و روش آشوبی معمولی بی عیب متمرکز شد .این معیار ها براساس سیستم رمزگذاری SEA انتخاب شدند که با تغییر در الگوریتم AES به دست آمده است. ما بررسی کردیم که روش آن ها زمان اجرا را تا نصف کاهش می دهد، موقعیت در داده ی رمزگذاری شده بالاتر از ٪35 و کیفیت آنتروپی حدود 7/9892 است. بنابراین با توجه به این مقادیر ، ممکن است نتیجه گرفته شود که سطح امنیت سیستم ان ها در حد نرمال است.

"کومار" الگوریتم RC4 را برای افزایش امنیت RC4 در برابر حملات بهبود داده است. سپس RC4 بهبود یافته با روش رمزگذاری عکس انتخابی به کار گرفته شد. روش رمزگذاری عکس انتخابی شامل دو مرحله است: 1) برای انتخاب سطح عکس معنی دار و 2) برای رمزگذاری مکان های انتخاب عکس. در قضیه ی روش انتخابی می توان گفت که امنیت

پایین تر و رمزگذاری در دوره ی زمانی کوتاه تر قابل دست یابی است. با وجود این، با محل کوچکی روی عکس اصلی، که در آن رمزگذاری اجرا شده است، امنیت عکس ممکن است مبادله شود.

"راد و همکارانش" روش رمز گذاری عکس دیگری به وسیله ی ترکیب چند الگوریتم ایمن ، Blowfish، AES، Serpen و RC6 پیشنهاد دادند. این استراتژی قفل های حساس را کد گذاری می کند در حالی که قفل غیر حساس با استفاده از چهار نوع الگوریتم ممتاز مجددا اسکن می شود. هر قفل به وسیله ی روش تشخیص لبه به صورت قفل

های معنا دار و بی معنا نام گذاری می شوند. در فاز رمز گذاری روش ترکیبی برای اطمینان از این که سطوح امنیت مختلفی برای قفل به دست می آید،انجام می شود. سیستم پیشنهادی سطوح مختلفی از امنیت برای قفل های مختلف با توجه به هزینه ی محاسبات ارائه می دهد. این استراتژی سطح بالایی از امنیت را ایجاد می کند در نتیجه برای مهاجم سخت است تا رمز عکس را بشکند.

"پان دورانکا و نون کوکار" دو سیستم رمزگذاری عکس انتخابی پیشنهاد دادند. به وسیله ی سیستم اول ، عکس به قفل هایی تفکیک می شود. قفل های انتخاب شده سپس به وسیله ی نقشه ی عکس، رمزگذاری می شوند که به عنوان ورودی به کار می رود تا قفل ها انتخاب شوند. رمزگذاری کامل قفل های انتخابی امکان پذیر است و هر قفل می تواند نقشه ی عکس را تفکیک کند. در سیستم دوم، موقعیت آیتم ها در عکس داده شده به طور طبیعی با استفاده از روش های مورفولوژی شناسایی می شود، که موقعیت های موضوعات عکس داده شده تعیین می شود. سپس رمزگذاری اطلاعات ساخته شده انجام شد وسپس روی تصویر اصلی منطبق شد. این دو روش برای اپلیکیشن های غیر معمول مثل عکس پزشکی وعکس ماهواه ایی به شدت مناسب است. این روش های به کار رفته وقتی محدوده یا موقعیت مورد نظر شناخته شده است اغلب ارزشمند خواهد بود.

3.2.2. محدوده فرکانس

"ردری جوس و همکارانش" یک روشی که مبتنی بر رمزگذاری رشته ی AES با استفاده از کدگذاری طول متغیر(VLC) بردار هافمن است، پیشنهاد دادند. برای شروع، عکس ورودی به قفل های 8×8 پیکسلی تقسیم بندی می شود. سپس، هر قفل ازمحدوده ی فضایی به محدوده ی فرکانس با استفاده از انتقال کسینوس گسسته (DCT) منتقل می شود. در مرحله ی بعد، یک فرآیند تدریجی روی عکس حاصل با استفاده از سیستم اسکن زیگزاگ منتقل می شود و نهایتا استراتژی رمزگذاری AES اعمال می شود. مزایای این روش که در رفرنس 29 آمده است عبارتند از امکان شناسایی یک یا دو بخش برای هر قفل 8×8 پیکسلی یا مونتاژ آن ها. این مطلب از این حقیقت ناشی می شود که ردری جوس و همکارانشAES را به عنوان بخشی از حالت CFB (قفل فیدبک رمزی) به کار می برند و آن را روی

هر قفل متصل می کنند. ذکر این نکته ضروری است که ROI باید در واحد قفل 8×8 پیکسلی به عنوان آرایش JPEGپیش فرض تعریف شده باشد. استراتژی آن ها به نظر می رسد یک فضای کلید یزرگ 2128 دارد که تاثیرپذیری بالای سیستم رمز گذاری برای یک تغییر کوچک در کلید رمز را نشان می دهد.

"او و همکرانش" استراتژی رمزگذاری انتخابی مبتنی بر بخش را ارائه دادند که اساسا برای رمزگذاری داده ی پزشکی به کار خواهد رفت. ابتدا، دو MSB با ناحیه ی مورد نظر (ROI) به ضرایب با استفاده از انتقال موجی تبدیل خواهد شد. سپس یک AES در حالت CFB مورد استفاده قرار می گیرد تا فقط بخش های معینی از داده ی قبلی را رمز گذاری کند. براساس این حقیقت، اندازه ی رشته ی بیتی رمزگذاری شده بدون تغییر باقی می ماند. نتایج تلاش آن ها نشان داد که این روش سطح امنیت پایینی ارائه می دهد.

" یاکالا و همکارانش" از انتقال DCT و روش رمزگذاری سبک وزن صعودی برای رمزگذاری قفل های انتخاب شده با لبه های معین استفاده کردند. تفکر پشت روش انتخابی آن ها رمزگذاری قفل های انتخاب شده با اطلاعات قاطع به وسیله ی استفاده از مقادیر محدود در گستره ی ویژه ایی است، در حالی که قفل های مربوط به محدوده های دیگر رمزگذاری نشده اند. اعتبار PSNR 14/46 دسی بل فراهم خواهد شد که مزاحم یا مهاجم نمی تواند کلید رمز مورد استفاده برای رمزگذاری را رمزگشایی کند.

"برهیمی و همکارانش" یک روش رمزگذاری انتخابی از طرح عکس مبتنی بر JPEG2000 پیشنهاد دادند که فقط کدقفل های متناظر با برخی زمینه های دقیق را رمز گذاری می کند. اجرای کدقفل های انتخاب شده در محدوده ی انتخابی صورت می گیرد تا امنیت را بالا برد. رمزگذاری متقارن AES با حالتCFB مورد استفاده قرار خواهد گرفت تا کد قفل های معاوضه شده را رمزگذاری کند. اندازه گیری داده ی پردازش شده در رمزگذاری و مراحل اجرا و رمزگذاری انتخابی با هم حداقل است. این الگوریتم با هر رمز استانداردی کار می کند و به هزینه ی محاسبات کمی نیاز دارد . محدوده ی رمزگذاری شده حدود 11/64 درصد است. وقتی محدوده ایی از تصویر اصلی در زمان کمی برای رمز گذاری کوچک باشد باز هم امنیت بالاست. عکس رمز گذاری شده از عکس اصلی مستقل خواهد بود به دلیل

اینکه PSNR مقدار کوچکی دارد، حدود 6/74 دسی بل که بازیابی عکس اصلی بدون داشتن کلید رمز را سخت می کند.

در رفرنس 88 ، یک روش جدید با استفاده از سه سطح اجرا در قفل های انتخاب شده و ضرایب محدوده ی انتقال چند جمله ایی ارتوگونال معرفی شده است. عکس اصلی در ابتدا به دو قفل 4×4 پیکسلی تقسیم شده و در سه زمان بازچینی می شوند. در ابتدا، انتقال مبتنی بر چند جمله ایی ارتوگونال (OPT) به همه ی بیت های انتخابی بازچینی شده اعمال شده، سپس قفل ضرایب OPT به یک سکوئنس زیگزاگ یک بعدی تبدیل خواهد شد. قفل های بازآرایی شده طبق سکوئنس پزدو رندوم ایجاد شده با استفاده از زیر کلید رمزی به عنوان پایه انتخاب می شوند. نهایتا، قفل ها به زیر مجموعه هایی تقسیم شده و بازآرایی می شوند. این در هم آمیختگی وضعیت فضایی محتوا را تغییر می دهد و برای یک مهاجم سخت تر است تا آن را بشکند. OPT به صورت انتقال صحیح در زمان محاسبه ی کم شکل می گیرد . برای کاهش زمان رمزگذاری بازچینی بیت ها، ضرایب و قفل ها کنترل می شوند. OPT برای یک فضای کلید بزرگ در نظر گرفته می شود که شانس خطر را افزایش می دهد و با مقدار ضریب هم بستگی گزارش شده ی 0/0366 ، OPT در مقابل حملات مختلف قوی است. به علاوه تکنیک گزارش شده برای اندازه ی استاندارد 25 درصد برای بخشی از رمزگذاری مورد استفاده قرار گرفت که نشان می دهد عکس رمزگذاری شده از تصویر اصلی مستقل است.

" درکول کارنی و همکارانش" یک روش رمز گذاری انتخابی پیشنهاد دادند که در این روش 5 سطح انتقالات موجی برای تجزیه ی عکس ورودی به وسیله ی اعمال بانک های فیلتر موجی به کار می رود. برای تهیه کردن یک عکس با ساختار سلسله مراتبی ، فیلترهای باند با عبور بالا و باند با عبوری پایین مورد استفاده قرار گرفت تا هر ساختار معنی متفاوتی داشته باشد. طبق سیستم بصری انسانی (HVS) ورژن پایین تر عکس اصلی به وسیله ی روش پیشنهادی سطح کافی از شفافیت ارائه می دهد. این سیستم ضریب هم بستگی بالایی از زیر باندها انتخاب می کند تا امنیت با شفافیت کنترل شود. بنابراین، PSNR اعتبار کمی دارد، حدود 3/448 دسی بل که برای مهاجم سخت است تا بدون داشتن کلید رمز، عکس اصلی را بازیابی کند.

" یونیس و همکارانش" یک روش رمز گذاری جدید پیشنهاد دادند که در آن بخش مهمی از دو زیر باند سطح عکس به وسیله ی به کار بردن ابزار C فازی (FCM)و تکنولوژی پیشرفته ایی برای آزمایش اجرای رمز مورد استفاده قرار خواهد گرفت. فقط ٪25-6/25 از داده های اصلی با کاهش چشمگیری در زمان رمزگذاری و رمز گشایی، رمز گذاری شدند. الگوریتم رمزگذاری عبارت است از انتقال فشرده ی موجی ، فرآیند تدریجی به وسیله ی FCM ، اجرای رمز و محاسبات کدسازی برای عکس های زیر باند دو سطحه . استراتژی رمزگذاری جزئی پیشنهاد شده بسیار سریع و ایمن خواهد بود. موجی بودن مبتنی بر بردار تدریجی و اجرا برای داشتن سطح نرمالی از امنیت مناسب تر است زیرا PSNR عکس بازسازی شده گران است. اما وقتی کیفیت رمزگذلری افزایش یابد ، هم PSNR و هم زمان اجرا هم افزایش خواهد یافت. می توان مشاهد کرد که فضای کلید بزرگ خطر و امکان حمله ی مهاجم را کاهش می دهد.

" فلای و همکارانش" یک روش رمزگذاری جزئی عکس کارآمد پیشنهاد دادند و سه سطح از انتقال موجی گسسته (DWT) به همراه رمز AES و رمز رشته ایی را به کار بردند . در این روش، عکس با استفاده از فیلتر صاف کننده با در نظر گرفتن نقاط اتصال عکس رمزی صاف می شود آن قدر که قابلیت مناطق رمزگذاری شده در عکس کاهش یابد. مشاهده خواهد شد که عکس بازسازی شده به عکس اصلی بسیار نزدیک است. روش آن ها مناطق رمزگذاری شده را تا 1/5625 درصد کاهش داد که در نتیجه زمان اجرای فرآیند رمزگذاری کاهش می یابد. می توان گفت که رمزگذاری بخش کوچکی، هم بستگی عکس رمزی را افزایش می دهد که ممکن است عکس را مستعد خطر کند. علاوه بر این دیده شده است که AES که به عنوان فضای کلید اصلی شناخته شده است، فضای کلیدی حدود 2128 به وجود می آورد و وقتی به رمز 216فضای کلید متصل می شود، فضای کلید گران اجتناب ناپذیر است. بنابراین باید گفت که با این اندازه ی فضای کلید بخش مهمی از اطلاعات رمز گذاری شده ایمن است.

" ریچارد و همکارانش" یک الگوریتم رمز گذاری منطقه ایی انتخابی پیشنهاد دادند. الگوریتم آن ها مورد استفاده قرار گرفت تا به طور جزئی عکس اصلی را به وسیله ی اجرای ضرایب در محدوده ی DCT رمز گذاری کند. الگوریتم شناسایی لبه مورد استفاده قرار گرفت تا مناطق عکس را تفکیک کند. این الگوریتم، آستانه را به کار می برد تا مناطق ضخیم عکس را از مناطق ضعیف تر تفکیک کند. سپس فیلتر میانی به عکس حاصل متصل شده تا ترکیبات اغتشاشی

در عکس را کاهش دهد . سپس استراتژی رمز گذاری اصلی ، که ویژگی های فشرده سازی مربوط به شکل انتقال کسینوس متغیر را به کار می برد، در محدوده ی DCT متصل شد. محدوده ی رمزگذاری شده با مناطق چندگانه برای رمز گذاری عکس حدود ٪10 است که ممکن است امنیت داده ی رمز گذاری شده را افزایش دهد.

" ساسید هاران و فیلیپ" یک طرح رمز گذاری عکس جزئی سریع با استفاده از رمز رشته ایی RC4 و انتقال موجی گسسته پیشنهاد دادند. در روش پیشنهادی آن ها رمز گذاری در پایین ترین پهنای فرکانس با استفاده از رمز رشته ایی اجرا شد. منظور اصلی آن ها برای استفاده از رمز رشته ایی، نگه داری همه ی اطلاعات عکس بود. باید گفت که ممکن است، استفاده از رمزهای رشته ایی زمان بیشتری صرف کند زیرا به طور معمول در یک زمان یک بایت را رمز گذاری می کند. XOR مورد استفاده قرار خواهد گرفت تا رشته های کلید و عکس اصلی که در گذشته به وسیله ی اعداد تصادفی تولید شده است را متصل کند. در یک نقطه وقتی لبه ها روبه روی هم قرار می گیرند ، از یک الگوریتم در هم آمیخته استفاده می شود. زمان رمز گذاری به وسیله ی رمز گذاری فقط یک باند فرکانس هر عکس کاهش می یابد و یک حالت غیر نرمال از امنیت به وسیله ی باقی ماندن در هم آمیختگی به دست می آوردکه فضای کلید آن حدود 2256 تخمین زده شده است. می توان دید آنتروپی عکس رمز گذاری شده ی حاصل حدود 4/7807 است، بنابراین مزاحم باید یک مرحله ی تجزیه ی بیشتر انجام دهد تا عکس رمز گذاری شده را رمز گشایی کند. هم زمان الگوریتم در مقابل حملات، قوی است زیرا PSNRاعتبار بالایی دارد، حدود 20/7056 دسی بل.

" کوپو سامی و دامودارن" یک طرح بهینه ی رمز گذاری جزئی عکس با استفاده از ضرایب مهم عکس منتقل شده ارائه دادند که به وسیله ی به کار گرفتن روش بهینه سازی هجوم ترکیبات (PSO) با محدوده ی daubechies4 برای رمز گذاری انتخاب شد. مشاهده شد که فضای کلید 2256 است و فضای کلید به وسیله ی افزایش تعداد اجرا برای هر دور اجرا افزایش می یابد و به سطح امنیت نرمال می رسد. محدوده ی رمز گذاری شده از عکس حدود ٪33 است که نرخ پایینی خواهد بود و سرعت متوسط رمز گذاری را نشان می دهد.

در رفرنس 59 یک روش پیشنهاد شده است که نقشه ی آرنولد را در فرکانس پایین زیر باند عکس منتقل شده ی DCTبرای رمز گذاری به کار می گیرد. مهم ترین ایده ی آن ها برای انتخاب فرکانس پایین زیر باند از عکس منتقل

شده ی DCT مربوط به این حقیقت است که سیستم بصری انسانی (HVS) بیشتر کشش اطلاعات در فرکانس های پایین تر را نسبت به اطلاعات در فرکانس بالاتر دارد و اطلاعات مهم مثل موضوع ، شکل و غیره در فرکانس پایین زیر باند ارائه می شود. در حالی که اطلاعات جزئی بیشتر در زیر باندهای فرکانس بالاتر قرار دارد. استنتاج ما این است که چون فقط ضرایب DCT، زیر باندها ی فرکانس پایین تر رمز گذاری شده اند، احتمال پیش بینی اطلاعات رمز گذاری شده کاهش می یابد. این روش با نویز قوی مقابله می کند، چرا که برخی حوزه های یک عکس رمز گشایی شده حضور نویز را نشان می دهند.

طرح رمز گذاری عکس پیشنهاد شده روی انتقال Mellin کسری و روش بازیابی فاز متمرکز است. هر عکس ممکن است به عنوان متن رمزی در نظر گرفته شود. فضای حلقوی برگزیده از عکس ویژه ابتدا به وسیله ی انتقال Mellin کسری منتقل می شود. در نتیجه ی انتقال، کلید فاز می تواند به وسیله ی روش بازیابی فاز به عنوان بخشی از فضای فوریه ی کسری حاصل شود. طرح پیشنهاد شده می تواند نیروی انتقال را تقلیل دهد، فضای کلید را توسعه دهد و ممکن است رمز گذاری عکس به مقدار زیادی بسط داده شود. نتایج روش پیشنهاد شده قابلیت دست یابی و شایستگی طرح پیشنهادی را نشان می دهد.

روش جدید برای رمز گذاری به وسیله ی انتخاب فرکانس های بالاتر ویژه ی مربوط به ضرایب DCT که به عنوان مقادیر مشخصه گرفته می شود، رمز گذاری آن ها و قفل های رمز گذاری به دست آمده طبق سکوئنس بیتی پزدو رندوم در هم آمیخته است. رمز گذاری انتخابی یک روش جدید برای کاهش نیازهای محاسباتی برای حجم بزرگی از عکس هاست. رمز گذاری عکس سطح وسیعی از تحقیقات را پوشش می دهد. رمز گذاری اساسا با تبدیل داده یا اطلاعات از شکل اصلی اش به شکل دیگری که اطلاعات در آن قرار می گیرد، سر و کار دارد . حفاظت داده ی عکس از دسترسی بدون مجوز مهم است. رمز گذاری به کار گرفته می شود تا امنیت داده افزایش یابد. عکس رمز گذاری شده از هر نوع آنالیزهای رمزی ایمن است. در کار پیشنهادی ، عکس رمز گذراری شده به قفل های 8×8 تجزیه می شود. این قفل ها از محدوده ی فضایی به محدوده ی فرکانس به وسیله ی DCTانتقال می یابند. سپس ضرایب مثل ضرایب DCT مربوط به فرکانس های بالاتر قفل عکس رمز گذاری شده انتخاب می شوند. برای رمز گذاری ضرایب

DCTبه بیت پزدو رندوم متصل می شود. بیت پزدو رندوم به وسیله ی ثبت حرکت بازگشتی غیر خطی تولید می شود. بیت های تولید شده به وسیله ی ثبت حرکت بازگشتی غیر خطی قابل پیش بینی نیستند، در نتیجه آنالیزهای رمز سخت می شود. برای بالا بردن امنیت بیشتر، ضرایب DCT رمز گذاری نشده در هم آمیخته می شوند،چون بعضی اطلاعات ممکن است با ضریب هم بستگی DCT برای فرکانس پایین تر هم مرتب شوند. در حالی که ضرایب DCT انتخابی رمز گذاری شده به تنهایی رمز گذاری کاملی فراهم خواهد کرد. اما این ضرایب می توانند اطلاعات زیادی درباره ی عکس از دیگر ضرایب فراهم کرده و در اختیار مهاجم قرار دهند، به ویژه در عکس هایی که لبه های زیادی دارند.

استراتژی دیگر برای رمز گذاری عکس به وسیله ی فرکانس های بالاتر ویژه ی انتخابی از ضرایب DCT -که به صورت کیفیت های با علامت تجاری در نظر گرفته می شوند- بازچینی آن هاست. سپس قفل های باز چینی شده به وسیله ی بازآرایی بیت پزدو رندوم بازآرایی می شوند. رمز گذاری جزئی یک روش جدید برای کاهش شرایط محاسباتی در حجم بزرگی از عکس هاست. رمز گذاری عکس بخش وسیعی از آزمایش است. رمز گذاری اساسا با تغییر اطلاعات یا داده از ساختار اصلی و پنهان کردن آن ها در ساختارهای دیگر همراه است. بیمه ی اطلاعات عکس در مقابل دسترسی ها بهترین کار است. رمز گذاری مورد استفاده قرار می گیرد تا امنیت اطلاعات را فراهم کند. عکس کدگذاری شده از هر نوع آنالیزهای رمز نگاری ایمن است . در کار پیشنهاد شده، عکس کد گذاری شده به قفل های 8×8 تجزیه شده، این قفل ها از محدوده ی فضایی به وسیله ی DCT،به سطح بازگشت منتقل می شوند. سپس فقط ضرایب منتخب مثل ضرایب DCT مربوط به فرکانس های بالاتر قفل عکس بازچینی می شوند. برای رمز گذاری ، ضرایب DCT با بیت پزدو رندم XOR خواهد شد، بیت پزدو رندوم به وسیله ی ثبت حرکت بازگشتی غیر خطی تولید خواهد شد. بیت های تولید شده به وسیله ی ثبت حرکت بازگشتی غیر خطی نمی توانند پیش بینی شود زیرا انجام آنالیزهای رمزی سخت است. برای پیشرفت بیشتر امنیت، ضرایب کدگذاری نشده بازآرایی نمی شوند، زیرا بعضی داده ها هم ممکن است کنار گذاشته شوند. در حالی که بازچینی ضرایب DCT منتخب به تنهایی رمز گذاری کاملی ایجاد خواهد کرد، اما این

امکان را برای مهاجم فراهم نمی کند تا بتواند داده ایی درباره ی عکس از دیگر ضرایب بردارد، به ویژه در عکس هایی که لبه های زیادی دارند.

در رفرنس 98، یک روش سریع تر برای رمز گذاری عکس پیشنهاد شده است. اینجا نویسندگان از رمز گذاری کسری استفاده کردند تا زمان مورد نیاز برای رمز گذاری، بدون بازچینی کاهش دهد و به جای بازچینی کل عکس فقط بیت انتخابی از عکس بازچینی می شو.، این کار باعث می شود رمز گذاری سریع تر انجام شود و زمان لازم کاهش یابد. تراکم در این سیستم کنار گذاشته می شود زیرا تراکم ضرورتا فقط برای اولین عکس در نظر گرفته می شود. برای اضافه کردن امنیت بیشتر عکس در رمزنگاری ، در احیا باز چینی ضرایب بالاتر منتخب، همه ی ضرایب می توانند مخلوط شوند. با تفکر پشت بازچینی همه ی ضرایب در برابر هر نوع حمله ایی ایستادگی می کنند.

3.2.3 . قلمرو هیبریدی

" ین و گو" روش رمز گذاری جزئی پیشنهاد دادند که برای عکس های متراکم با دو گروه ویژه از الگوریتم های تراکم مناسب است: آ) الگوریتم های تراکم درخت چهارگانه و ب) الگوریتم های تراکم موجی مبتنی بر درخت های صفر.

یکی از نوشته هایی که شامل مزایای ترکیب محدوده های فضایی و فرکانس در روش رمز گذاری موفق است، مقاله ایی منسوب به " تانجا و همکارانش" می باشد. در کار آن ها موج کسری مورد استفاده قرار می گیرد تا فقط زیر باندهای معنادار را با استفاده از نقشه ی آرنولد و نقشه ی منطقی کدگذاری کند. آن ها اغلب بخش مهمی از عکس در محدوده ی فضایی را رمز گذاری می کند و سپس بخش های ناچیز به طور جزئی کدگذاری می شود. قبل از پردازش فرکانس یک شاخص Prewitt مورد استفاده قرار گرفت تا لبه ها در عکس را حذف کند و بخش معنی دار عکس را حفظ کند. آنالیزهای امنیت روش پیشنهادی آن ها نشان می دهد که با این روش درک بهتر و رمزنگاری ایمن تری فراهم می شود زیرا زمان محاسبات کمتری برای کدگذاری عکس لازم است. نتیجه گرفته شده است که عکس رمز گذاری شده با استفاده از استراتژی مستقل از عکس اصلی و در محدوده ی هیبریدی به دست می آید که تنظیم آن سخت است.

یک مفهوم جدید که دست کاری فاز و رمز گذاری علامت در سیستم رمزگذاری جزئی عکس را ترکیب می کند به وسیله ی " پارامش چری و همکارانش" ارائه شد. روش رمز گذاری آن ها شامل دو مرحله است: در مرحله ی اول ، فاز و اندازه ی عکس ورودی با استفاده از انتقال فوریه ی سریع (FFT) تعیین می شود . سپس جز فاز مربوط به عکس از انتقال فوریه ی سریع معکوس (IFFT) با ورژن عکس متعادل در هم آمیخته می شود. در مرحله ی دوم ، عکس تغییر یافته به طور جزئی با استفاده از رمزگذاری علامت، رمز گذاری می شود. رمز گذار علامت به وسیله ی استخراج بیت های شاخص از عکس تغییر یافته در عکس رمز گذاری شده به طور جزئی به دست می آید. می توان نتیجه گرفت که استراتژی پیشنهادی آن ها سریع است و برای داده ی رمز گذاری شده امنیت پایینی دارد. علاوه بر این روشن است که عکس رمز گذاری شده مستقل از عکس اصلی است و برای مزاحم سخت خواهد بود تا کلید رمز داده شده را بداند. ضمن آن که مقدار میانه ایی آنتروپی دارد و بنابراین مستعد خطر بیشتری است.

" کارل مارتین و همکارانش" یک سیستم رمز گذاری عکس جزئی با استفاده از تراکم color-SPIHT پیشنهاد دادند. رمز گذاری عکس فقط به وسیله ی بازچینی ضرایب موجی فردی برای تکرارهای k از الگوریتم C-SPIHT فراهم می شود. انتقال k نوسانی بالای سر و سطح امنیت فراهم می شود.

4. نتایج

در این مقاله، بخش های زیادی از روش های رمز گذاری عکس رایج ارائه شده و بررسی شدند. در این گزارش مروری ، ابتدا مسائل موجود در الگوریتم های رمز گذاری عکس بررسی شد که این حقیقت را آشکار کرد که ایده آل ترین روش برای امنیت اطلاعات مثل عکس ها بازچینی متوالی بیت های صوتی و تصویری با استفاده از سیستم های سریع رمزنگاری مرسوم است. یک بخش منتخب از رشته ی بیتی عکس، در حافظه ذخیره می شود تا انجام محاسبات را کاهش دهد و سطح بالایی از امنیت را حفظ کند . تعداد زیادی از طرح های پیشنهادی می توانند به طور مناسب اجرا شود تا به سطح مورد نظر از امنیت برسد چرا که ممکن است اپلیکیشن های کشف شده کیفیت مورد نظر سطح امنیت را کاهش دهند. اما فقط تعدادی از استراتژی های پیشنهادی ضمانت می کنند که امنیت قابل قبولی ایجاد کنند ، که

ضمانت شرط اصلی استفاده از یک استراتژی در اپلیکیشن های محیطی زیادی است. دوما، الگوریتم های رمز گذاری عکس زیادی را بررسی و آن ها را به صورت روش های رمز گذاری عکس جزئی و کلی در محدوده های فضایی، فرکانس و هیبریدی، دسته بندی کردیم. در فرآیند این مطالعه، موارد کمی وجود داشت که در آن ها یک طرح رمز گذاری کلی میزان بالایی از امنیت اطلاعاتی کدگذاری شده را ضمانت کند، زیرا روش های کلی همه ی عکس را کد گذاری می کنند و بنابراین به زمان بیشتری نیاز دارند. در روش های رمز گذاری انتخابی عکس ، فقط یک موقعیت یا برخی بخش های عکس بازچینی می شوند، بنابراین زمان کدگذاری در این روش نسبت به استراتژی های کلی کمتر است و در نتیجه طرح رمزگذاری جزئی برای اپلیکیشن های ثابت مناسب تراست. بنابراین طرح رمز گذاری جزئی عکس ارائه شد تا زمان رمز گذاری کاهش داده شود. رسیدن به روش رمز گذاری که امنیت را با زمان انتقال برای اپلیکیشن های در حال پیشرفت تعدیل می کند هنوز یک چالش برای محققلن در رمزگذاری عکس است. از طرف دیگر، بعضی عناصر کلیدی، برای مثال ، مرتب کردن اطلاعات برای کد گذاری ، نرخ اطلاعاتی که باید تضمین شود و اندازه گیری هایی که باید تنظیم شود تا اطلاعات محافظت شود وقتی شامل وضعیتی از روش رمزگذاری عکس پیوسته باشند، ممکن است جواب قابل قبولی برای مسئله ی رمز گذاری عکس در حال پیشرفت باشد.

References

1. Shannon, C. E. (1948). The mathematical theory of communication. *The Bell System Technical Journal, 27*, 379–423.
2. Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal, 28*, 656–715.
3. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Applied cryptography*. Boca Raton: CRC.
4. Ding, W., Yan, W.-Q., & Qi, D.-X. (2000). *A novel digital hiding technology based on Tangram Encryption. IEEE Proceedings of on NEWCAS* 2005, *and Conways Game. Proceeding of* 2000 *International Conference on Image Processing* (Vol. 1, pp. 601–604), September 2000.
5. Zhao, X.-F. (2003). Digital image scrambling based on the Baker's transformation. *Journal of Northwest Normal University (Natural Science), 39*(2), 26–29.
6. Bao, G.-J., Ji S.-M., & Shen J.-B. (2002). Magic cube transformation and its application in digital image encryption. *Computer Applications*, *22*(11), 23–25.
7. Guibin Z, Changxiu C, Hu Zhongyu, et al. (2003). An image scrambling and encryption algorithm based on affine transformation. *Journal of Computer-Aided Design & Computer Graphics*, *15*(6), 711–715.
8. Jawad, L. M., & Sulong, G. B. (2013). A review of color image encryption techniques. *International Journal of Computer Science Issues, 10*(6), 266–275.
9. Sharma, M., & Kowar, M. K. (2010). Image encryption techniques using chaotic schemes: a review. *International Journal of Engineering Science and Technology, 2*, 2359–2363.
10. Li, C.-G., Han, Z.-Z., & Zhang, H.-R. (2002). Image encryption techniques: A survey. *Journal of Computer Research and Development, 39*(10), 1317–1324.
11. Rober, A., & Matthews, J. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, *XIII*(1), 29–42.
12. Habutsu, T., Nishio, Y., Sasase, I., & Mori, S. (1990). A secret key cryptosystem using a chaotic map. *Transactions of the IEICE*, *E*73(7), 1041–1044.
13. Schwartz, C. (1991). A new graphical method for encryption of computer data. *Cryptologia, 15*(1), 43–46.
14. Bourbakis, N., & Alexopoulos, C. (1992). Picture data encryption using scan patterns. *Pattern Recognition, 25* (6), 567–581.
15. Kuo, C. J. (1993). Novel image encryption technique and its application in progressive transmission. *Journal of Electronic Imaging, 2*(4), 345–351.
16. Chang, K.C., & Liu, J.L. (1994). An image encryption scheme based on quad-tree compression scheme. In *Proceedings of the 1994 International Computer Symposium*, *Taiwan*, (pp. 230–237).
17. Alexopoulos, C., Bourbakis, N., & Ioannou, N. (1995). Image encryption method using a class of fractals. *Journal of Electronic Imaging, 43*, 251–259.
18. Yang, H.-G., & Kim, E.-S. (1996). Practical image encryption scheme by real-valued data. *Optical Engineering, 35*(9), 2473–2478.
19. Scharinger, J., & Pichler, F. (1996). Image encryption based on chaotic maps. *Proceedings of the 20th workshop of the Austrian Association for Pattern Recognition* (*OAGM/ AAPR*) *on Pattern recognition 1996* (pp. 159–170).
20. Fridrich, J. (1997). Image encryption based on chaotic maps. *Proceedings of IEEE Conference on Systems*, *Man*, *and Cybernetics* (pp. 1105–1110).
21. Baptista, M. S. (1998). Cryptography with chaos. *Physics Letters A, 240*, 50–54.
22. Guo, J.-I., & Yen, J.-C. (1999). A new mirror-like image encryption algorithm and its VLSI architecture, Department of Electronics Engineering, National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China in 1999.
23. Yen, J.-C., & Guo, J.-I. (2000). New chaotic key-based design for image encryption and decryption. *IEEE International Symposium on ISCAS 2000*, *Geneva* (pp. IV-49–IV-52), May 2000.
24. Sobhy, M. I., & Shehata, A. R. (2001). Chaotic algorithms for data encryption. *IEEE Proceeding of ICASSP 2001*, (Vol. 2, pp. 997–1000), May 2001.
25. Masuda, N., & Aihara, K. (2002). Cryptosystems with discretized chaotic maps. *IEEE Transactions on Circuits*

and Systems I Fundamental Theory and Applications, *49* (*1*), 28–40.
26. Sinha, A., & Singh, K. (2003). A technique for image encryption using digital signature. *Optics Communications*, 1–6. Retrieved from www.elsevier.com/locate/optcom.
27. Sallen, M., Ibrahim, S., & Isnin, I. F. (2003). Enhanced chaotic image encryption algorithm based on Baker's map. *IEEE Proceedings of ISCAS 2003*, 2, II-508–II-511.
28. Shin, C.-M., Seo, D.-H., Chol, K.-B., Lee, H.-W., & Kim, S. J. (2003). Multilevel image encryption by binary phase XOR operations. *IEEE Proceedings in the year 2003*.
29. Belkhouche, F., & Qidwai, U. (2003). Binary image encoding using 1D chaotic maps. *IEEE Proceedings in the year 2003*.
30. Ying, W., DeLing, Z., Lei, J., et al. (2004). The spatial-domain encryption of digital images based on high-dimension chaotic system. *Proceedings of 2004 IEEE Conference on Cybernetics and Intelligent Systems*, *Singapore*, December 2004 (pp. 1172–1176).
31. Zhang, M.-R., Shao, G.-C., & Yi, K.-C. (2004). T-matrix and its applications in image processing. *IEEE Electronics Letters*, *40*(25), 1583–1584.
32. Deng, S., Zhang, L., & Xiao, D. (2005). Image encryption scheme based on chaotic neural system. In J. Wang, X. Liao, & Z. Yi (Eds.) *Advances in neural networks*, ISNN 2005, LNCS 3497 (pp. 868–872).
33. Gu, G., & Han, G. (2006). An enhanced chaos based image encryption algorithm. *IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control* (*ICICIC'06*) *in 2006*.
34. Xiao, H.-P., & Zhang, G.-J. (2006). An image encryption scheme based on chaotic systems. *IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics*, *Dalian*, *13–16 August 2006*.
35. Nien, H. H., Huang, W. T., Hung, C. M., Chen, S. C., Wu, S. Y., Huang, C. K., et al. (2009). Hybrid image encryption using multi-chaos-system. In *7th International Conference on Information, Communications and Signal Processing* (*ICICS*), *December 2009* (pp. 1–5).
36. Rhouma, R., Arroyo, D., & Belghith, S. (2009). A new color image cryptosystem based on a piecewise linear chaotic map. In *6th International Multi-Conference on Systems, Signals and Devices*, *March 2009*, (pp. 1–6).
37. Ahmad, M., & Alam, M. (2009). A new algorithm of encryption and decryption of images using chaotic mapping. *International Journal on Computer Science and Engineering, 2*(1), 46–50.
38. Wei, W., Fen-lin, L., Xinl, G., & Yebin, Y. (2010). Color image encryption algorithm based on hyper chaos. In *2nd IEEE International Conference on Information Management and Engineering*, *2010* (pp. 271–274).
39. Kamali, M. R., Hossein, S., Shakerian, R., & Hedayati, M. (2010). A new modified version of advanced encryption standard based algorithm for image encryption. *International Conference on Electronics and Information Engineering* (*ICEIE*), *2010*, *1*(Iceie), 141–145.
40. Aihong, Z., Lian, L., & Shuai, Z. (2010). Research on method of color image protective transmission based on logistic map. In *International Conference on Computer Application and System Modeling* (*ICCASM*), *Oct. 2010*, Vol. 9, No. Iccasm, pp. 266–269.
41. Rodriguez-Sahagun, M. T., Mercado-Sanchez, J. B., Lopez-Mancilla, D., Jaimes-Reategui, R., & Garcia-Lopez, J. H. (2010). Image encryption based on logistic chaotic map for secure communications. *IEEE Electronics, Robotics and Automotive Mechanics Conference*, *Sep. 2010*, (pp. 319–324).
42. Mastan, J. M. K., Sathishkumar, G. A., & Bagan, K. B. (2011). A color image encryption technique based on a substitution–permutation network. *Advances in Computing and Communications, 4*, 524–533.
43. Pareek, K. K. S., Narendra K, & Patidar, V. (2011). A symmetric encryption scheme for colour BMP images. *International Journal of Computer Applications*, *Special Issue on Network Security and Cryptography*, 42–46.
44. Abugharsa, A. B., & Almangush, H. (2011). A new image encryption approach using block-based on shifted algorithm. *International Journal of Computer Science and Network Security (IJCSNS), 11*(12), 123–130.
45. Yadav, R. S., Beg, M. H. D. R., & Tripathi, M. M. (2013). Image encryption techniques: A critical comparison. *International Journal of Computer Science Engineering and Information Technology Research, 3*(1), 67–74.
46. Zhang, G., & Liu, Q. (2011). A novel image encryption method based on total shuffling scheme. *Optics Communication, 284*, 2775–2780.
47. Eslami, Z., & Bakhshandeh, A. (2013). An improvement over an image encryption method based on total shuffling. *Optics Communications, 286*, 51–55.
48. Ding, X., & Chen, G. (2014). Optical color image encryption using position multiplexing technique based on phase truncation operation. *Optics & Laser Technology, 57*, 110–118.
49. Zhang, Y., & Xiao, D. (2014). An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. *Communications in Nonlinear Science and Numerical Simulation, 19*, 74–82.
50. Sinha A., Singh, K. (2013). Image encryption using fractional Fourier transform and 3D Jigsaw transform. Retrieved from http://pdf-world.net/pdf-2013/Image-encryption-using-fractional-Fourier-transform-and-3D-Jigsaw-transform-pdf.pdf.
51. Zhou, N., Wang, Y., Gong, L., Chen, X., & Yang, Y. (2012). Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. *Optics & Laser Technology, 44*(7), 2270–2281.
52. Abuturab, M. R. (2012). Securing color information using Arnold transform in gyrator transform domain. *Optics and Lasers in Engineering, 50*(5), 772–779.
53. He, Y., Cao, Y., & Lu, X. (2012). Color image encryption based on orthogonal composite grating and double random phase encoding technique. *Optik (International Journal for Light and Electron Optics), 123*(17), 1592–1596.
54. Chen, H., Du, X., Liu, Z., & Yang, C. (2013). Color image encryption based on the affine transform and gyrator transform. *Optics and Lasers in Engineering, 51* (6), 768–775.
55. Sui, Liansheng, & Gao, Bo. (2013). Single-channel color image encryption based on iterative fractional Fourier transform and chaos. *Optics & Laser Technology, 48*, 117–127.

56. Zhang, Y., Xiao, D., Wen, W., & Tian, Y. (2013). Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform. *Optics & Laser Technology, 54*, 1–6.
57. Liu, S., & Sheridan, J. T. (2013). Optical encryption by combining image scrambling techniques in fractional Fourier domains. *Optics Communications, 287*, 73–80.
58. Liu, Z., Li, S., Liu, W., Wang, Y., & Liu, S. (2013). Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. *Optics and Lasers in Engineering, 51*, 8–14.
59. Li, H., Wang, Y., Yan, H., Li, L., Li, Q., & Zhao, X. (2013). Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform. *Optics and Lasers in Engineering, 51*, 1327–1331.
60. Sui, L., Xin, M., Tian, A., & Jin, H. (2013). Single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain. *Optics and Lasers in Engineering, 51*, 1297–1309.
61. Kumar, M., Mishra, D. C., & Sharma, R. K. (2014). A first approach on an RGB image encryption. *Optics and Lasers in Engineering, 52*, 27–34.
62. Liu, Z., Zhang, Y., Li, S., Liu, W., Liu, W., Wang, Y., et al. (2013). Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains. *Optics & Laser Technology, 47*, 152–158.
63. Kong, Dezhao, & Shen, Xueju. (2014). Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. *Optics & Laser Technology, 57*, 343–349.
64. Ran, Q., Zhao, T., Yuan, L., Wang, J., & Lei, X. (2014). Vector power multiple-parameter fractional Fourier transform of image encryption algorithm. *Optics and Lasers in Engineering, 62*, 80–86.
65. Qin, Y., Jiang, H., & Gong, Q. (2014). Interference-based multiple-image encryption by phase-only mask multiplexing with high quality retrieved images. *Optics and Lasers in Engineering, 62*, 95–102.
66. Chen, J-x, Zhu, Z-l, Fu, C., Zhang, L-b, & Yu, H. (2015). Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains. *Optics and Lasers in Engineering, 66*, 1–9.
67. Yu, Z., Zhe, Z., Haibing, Y., Wenjie, P., & Yunpeng, Z. (2010). A chaos-based image encryption algorithm using wavelet transform. In *2nd International Conference on Advanced Computer Control, March 2010, Vol. 2, No. 4*, (pp. 217–222).
68. El-Latif, A., Niu, X., & Amin, M. (2012). A new image cipher in time and frequency domains. *Optics Communications, 285*(21–22), 4241–4251.
69. Zhou, N., Zhang, A., Zhen, F., & Gong, L. (2014). Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optics & Laser Technology, 62*, 152–160.
70. Zhang, X., Zhu, G., Ma, S. (2012). Remote-sensing image encryption in hybrid domains. *Optics Communications, 285*, 1736–1743.
71. H. B. Kekre, Tanuja Sarode, Pallavi N. Halarnkar, Debkanya Mazumder, Image Encryption using Hybrid Transform Domain Scrambling of Coefficients, International Journal of Advance Research in Computer Science and Management Studies 2 (6) (2014).
72. Shubhangini, P., Nichat, S. S., & Sikchi, M. E. (2013). Image encryption using hybrid genetic algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*, 427–431.
73. Krishnamoorthi, R., Murali, P. (2012). A new hybrid-domain image encryption based on chaos with discrete cosine transform. *4th International Conference on Electronics Computer Technology, IEEE 2012*.
74. Ramahrishnan, S., Elakkiya, B., Geetha, R., Vasuki, P., Mahalingam, S. (2014). Image encryption using chaotic maps in hybrid domain. *International Journal of Communication and Computer Technologies, 2*(5), 44–48.
75. Suresh, V., & Madhavan, C. E. V. (2012). Image encryption with space-filling curves. *Defence Science Journal, 62*(1), 46–50.
76. Rodrigues, J. M., Puech, W., & Bors, A. G. (2006). A selective encryption for heterogeneous color JPEG images based on VLC and AES stream cipher. *3rd European Conference on Colour in Graphics, Imaging and Vision (CGIV'06), June 2006, Vol. 1*, (pp. 34–39).
77. van Droogenbroeck, M. & Benedett, R. (2002). Techniques for a selective encryption of uncompressed and compressed images. *Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, September 9–11*.
78. Podesser, M., Schmidt, H.-P., & Uhl, A. (2002). Selective bitplane encryption for secure transmission of image data in mobile environments. *5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4–7*.
79. Rao, Y. V. S., Mitra, A., & Prasanna, S. R. M. (2006). A partial image encryption method with pseudo random sequences (pp. 315–325) (Lecture Notes in Computer Science, Vol. 4332) [International Commission on Intervention and State Sovereignty (ICISS)]. Berlin: Springer.
80. Wong, A., & Bishop, W. (2007). Backwards compatible, multi-level region-of-interest (ROI) image encryption architecture with biometric authentication. *International Conference on Signal Processing and Multimedia Applications, July 2007*, (pp. 324–329).
81. Ju-Young, Oh, Dong-Il, Yang, & Chon, K. H. (2010). "A Selective Encryption Algorithm Based on AES for Medical Information". *Healthcare informatics research, 16*(1), 22–29.
82. Kumar, P. (2012). RC4 enrichment algorithm approach for selective image encryption. *International Journal of Computer Science & Communication Networks, 2*(2), 181–189.
83. Rad, R. M., Attar, A., & Atani, R. E. (2013). A comprehensive layer based encryption method for visual data. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 6*(1), 37–48.
84. Panduranga, H. T., & Naveenkumar, S. K. (2013). Selective image encryption for medical and satellite images. *International Journal of Engineering and Technology (IJET), 5*(1), 115–121.

85. Ou, Y., Sur, C., & Rhee, K. H. (2007). Region-based selective encryption for medical imaging. *1st Annual International Workshop, 2007, Vol. 4427, No. 4613* (pp. 62–73).
86. Yekkala, A. K., Udupa, N., Bussa, N., & Madhavan, C. E. V. (2007). Lightweight encryption for images. *IEEE International Conference on Consumer Electronics, 3*, 1–2.
87. Brahimi, Z., Bessalah, H., Tarabet, A., & Kholladi, M. K. (2008). A new selective encryption technique of JPEG2000 code stream for medical images transmission. *5th International Multi-Conference on Systems, Signals and Devices, July 2008* (pp. 1–4).
88. Krishnamoorthi, R., & Malarchelvi, P. D. S. K. (2008). Selective combinational encryption of gray scale images using orthogonal polynomials based transformation. *International Journal of Computer Science and Network Security, 8*(5), 195–204.
89. Kulkarni, N. S., Raman, B., & Gupta, I. (2008). Selective encryption of multimedia images. *32nd National Systems Conference, Dec. 2008* (pp. 467–470).
90. Younis, H. A., Abdalla, T. Y., & Abdalla, A. Y. (2009). Vector quantization techniques for partial encryption of wavelet-based compressed digital images. *Iraqi Journal of Electrical and Electronic Engineering, 5*(1), 74–89.
91. Flayh, N. A., Parveen, R., & Ahson, S. I. (2009). Wavelet based partial image encryption. *International Multimedia, Signal Processing and Communication Technologies (IMSPCT), Mar. 2009* (pp. 32–35).
92. Metzler, R. E. L., & Agaian, S. S. (2010). Selective region encryption using a fast shape adaptive transform. *IEEE International Conference on Systems, Man, and Cybernetic (ICSMC), 2010* (pp. 1763–1770).
93. Sasidharan, S., & Philip, D. S. (2011). A fast partial encryption scheme with wavelet transform and RC4. *International Journal of Advances in Engineering & Technology (IJAET), 1*(4), 322–331.
94. Kuppusamy, K., & Thamodaran, K. (2012). Optimized partial image encryption scheme using PSO. In *International Conference on Pattern Recognition, Informatics and Medical Engineering, May 2012* (pp. 236–241).
95. Munir, R. (2012). Robustness analysis of selective image encryption algorithm based on arnold cat map permutation. In *Proceedings of 3rd Makassar International Conference on Electrical Engineering and Informatics, Nov. 2012*, (pp. 1–5).
96. Zhou, N., Liu, X., Zhang, Y., & Yang, Y. (2013). Image encryption scheme based on fractional Mellin transform and phase retrieval technique in fractional Fourier domain. *Optics & Laser Technology, 47*, 341–346.
97. Krikor, Lala, Baba, Sami, & Arif, Thawar. (2009). Zyad Shaaban image encryption using DCT and stream cipher. *European Journal of Scientific Research, 32*, 48–58.
98. Divya, V. V., Sudha S. K., & Resmy, V. R. (2012). Simple and secure image encryption. *International Journal of Computer Science, 9(6)*, 286.
99. Taneja, N., Raman, B., & Gupta, I. (2011). Combinational domain encryption for still visual data. *Multimedia Tools and Applications, 59*(3), 775–793.
100. Parameshachari P. B. D., Soyjaudah, K. M. S., & Devi K. A. S. (2013). Secure transmission of an image using partial encryption based algorithm. *International Journal of Computer Applications, 63*(16), 33–36.
101. Martin, K., Lukac, R., & Plataniotis, K. N. (2005). Efficient encryption of wavelet-based coded color images. *Pattern Recognition, 38*(7), 1111–1115.